# Εισαγωγή

*Όσο σημαντικές και αν είναι οι γενικές έννοιες και προτάσεις που απορρέουν από το σύγχρονο πάθος για αξιωματική θεμελίωση και γενίκευση, είμαι όμως πεπεισμένος ότι τα ειδικά προβλήματα με όλη την πολυπλοκότητά τους αποτελούν το σώμα και τη ψυχή των μαθηματικών…*

*Herman Weyl*

Οι σημειώσεις αυτές αποτελούν μια εισαγωγή στη Μεταθετική Άλγεβρα. Απευθύνονται στους φοιτητές του Μαθηματικού Τμήματος που γνωρίζουν τα βασικά στοιχεία από ομάδες, δακτύλιους και σώματα όπως αυτά εξετάζονται στο μάθημα "Βασική Άλγεβρα" και έχουν ετοιμαστεί για να καλύψουν τις ανάγκες του προπτυχιακού μαθήματος "Μεταθετική Άλγεβρα και Εφαρμογές".

Η ύλη που αναπτύσσεται αντιστοιχεί ουσιαστικά στα κεφάλαια 1-9 του κλασσικού συγγράμματος των Atiyah και Macdonald, Introduction to Commutative Algebra [1]. Έχουμε όμως προσθέσει στοιχεία Αλγεβρικής Γεωμετρίας και Αλγεβρικής Θεωρίας Αριθμών που αποτελούν άλλωστε ιστορικές πηγές της Μεταθετικής Άλγεβρας.

Έχει καταβληθεί ιδιαίτερη προσπάθεια οι κεντρικές ιδέες των 12 κεφαλαίων και οι αποδείξεις των θεωρημάτων να είναι κατανοητές από το φοιτητή χωρίς να χρειάζεται εξωτερική βοήθεια. Έτσι έχουμε συμπεριλάβει όλα όσα χρειάζονται από την Άλγεβρα στο Κεφάλαιο 0. Επίσης οι αποδείξεις δίνονται με κάθε πληρότητα, πράγμα που ίσως έρχεται σε αντίθεση με την αριστοτεχνική οικονομία του βιβλίου των Atiyah και Macdonald.

Ο χρονικός περιορισμός που υπάρχει σ' ένα εξαμηνιαίο μάθημα μας ανάγκασε να μην επεκταθούμε σε θέματα όπως τανυστικά γινόμενα, οι συναρτητές Ext και Tor, κανονικές ακολουθίες, θεωρία διάστασης, κ.ά. Όμως αναπτύσσονται συγκεκριμένα σημαντικά θέματα σε τέτοιο βάθος που πιστεύουμε ότι δίνουν μια ικανοποιητική πρώτη γεύση της Μεταθετικής Άλγεβρας. Τα κυριώτερα από αυτά

είναι: δακτύλιοι της Noether, δακτύλιοι του Artin, κανονικοποίηση της Noether, Nullstellensatz και γεωμετρικές εφαρμογές, τοπικοποίηση, πρωταρχική ανάλυση ιδεωδών και δακτύλιοι διακριτής εκτίμησης.

Εννοείται ότι ο φοιτητής θα πρέπει να επιχειρήσει πολλές από τις ασκήσεις, οι οποίες κυμαίνονται από πολύ εύκολες έως απαιτητικές. Μερικές χρησιμοποιούνται παρακάτω· αυτές σημειώνονται με αστερίσκο *.

Ολοκληρώνουμε την εισαγωγή με μια συντομότατη αναφορά στις ιστορικές πηγές της Μεταθετικής Άλγεβρας (και έτσι απαντάμε έμμεσα στο ερώτημα “γιατί να μελετήσει κανείς Μεταθετική Άλγεβρα”).

i) *Αλγεβρική Θεωρία Αριθμών*

Το 1847 ο Lamé ανακοίνωσε ότι “απέδειξε” το τελευταίο θεώρημα του Fermat: για $n \geq 3$ η Διοφαντική εξίσωση $x^n + y^n = z^n$ δεν έχει μη τετριμμένες λύσεις. Θέτοντας $\zeta = \text{συν}\frac{2\pi}{n} + i\text{ημ}\frac{2\pi}{n} \in \mathbb{C}$ παρατήρησε ότι η παραγοντοποίηση

$$(x + y)(x + \zeta y)\cdots(x + \zeta^{n-1}) = z^n \qquad (1)$$

στο $\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots + a_r\zeta^r \mid a_i \in \mathbb{Z}\}$ οδηγεί στο εξής συμπέρασμα: αν τα $x$ και $y$ δεν έχουν μη τετριμμένους κοινούς διαιρέτες, τότε το ίδιο συμβαίνει ανά δύο για τους παράγοντες $x + y, x + \zeta y, ..., x + \zeta^{n-1}y$· Από την (1) συμπέρανε ότι κάθε παράγοντας $x + \zeta^i y$ είναι $n$-στή δύναμη στο $\mathbb{Z}[\zeta]$. Συνεχίζοντας από εκεί έφθασε σε άτοπο.

Όμως αμέσως ο Liouville επεσήμανε το λάθος: για να καταλήξει κάποιος στο συμπέρασμα ότι κάθε $x + \zeta^i y$ είναι $n$-στη δύναμη με τον τρόπο του Lamé, θα έπρεπε να ισχύει η *μοναδικότητα* της παραγοντοποίησης στο $\mathbb{Z}[\zeta]$. Λίγο αργότερα ο Kummer έδειξε ότι αυτή δεν ισχύει γενικά: $n = 23$ είναι η πρώτη αρνητική περίπτωση.

Η προσπάθεια αποκατάστασης οδηγεί στη δημιουργία του κλάδου της Μεταθετικής Άλγεβρας: ο Dedekind εισήγαγε την έννοια του ιδεώδους και απέδειξε ότι σε δακτύλιους όπως ο $\mathbb{Z}[\zeta]$ ισχύει η μοναδικότητα παραγοντοποίησης ιδεωδών. Λίγο αργότερα ο E. Lasker θεώρησε το αντίστοιχο πρόβλημα για πολυωνυμικούς δακτυλίους. Εισήγαγε μια ασθενέστερη

παραγοντοποίηση σε αυτούς (πρωταρχική ανάλυση) και απέδειξε τη μοναδικότητα (Κεφάλαιο 11). Γύρω στο 1920 η E. Noether ενοποίησε τα προηγούμενα αποτελέσματα, τα γενίκευσε σημαντικά και τα έθεσε σε αξιωματική βάση αναγνωρίζοντας το θεμελιώδη ρόλο που παίζει η συνθήκη της αύξουσας αλυσίδας ιδεωδών που η ίδια εισήγαγε (Κεφάλαιο 4). Σημειώνεται έτσι η απαρχή της σύγχρονης Μεταθετικής Άλγεβρας.

*ii) Αλγεβρική Γεωμετρία*

Το θεμελιώδες θεώρημα της Άλγεβρας περιγράφει μία σύνδεση μεταξύ της Άλγεβρας και της Γεωμετρίας: ένα πολυώνυμο πάνω από το $\mathbb{C}$ μιας μεταβλητής (αλγεβρικό αντικείμενο) προσδιορίζεται μονοσήμαντα (με προσέγγιση αριθμητικού πολλαπλασίου) από το σύνολο των ριζών του μαζί με τις πολλαπλότητες (γεωμετρικό αντικείμενο). Το Nullstellensatz επεκτείνει αυτή τη σύνδεση σε πολυώνυμα πολλών μεταβλητών. Για να γίνουμε πιο κατανοητοί χρειαζόμαστε πρώτα κάποιους ορισμούς.

Έστω *k* ένα σώμα. Μια ομοπαραλληλική πολλαπλότητα $V(J)$ είναι (για μας) το σύνολο κοινών ριζών στο $k^n$ ενός συνόλου πολυωνύμων $J \subseteq k[x_1,...,x_n]$. Μπορούμε να αντικαταστήσουμε το $J$ με το ιδεώδες που αυτό παράγει χωρίς να αλλάξει η ομοπαραλληλική πολλαπλότητα. Κατά συνέπεια υποθέτουμε ότι το $J$ είναι ιδεώδες. Αν $X \subseteq k^n$ είναι μια ομοπαραλληλική πολλαπλότητα, με $I(X)$ συμβολίζουμε το ιδεώδες των πολυωνύμων $f \in k[x_1,...,x_n]$ που μηδενίζονται στο *X*.

Έτσι έχουμε αντιστοιχίες: ιδεώδη του $k[x_1,...,x_n]$ (αλγεβρικά αντικείμενα) $\underset{I}{\overset{V}{\rightleftarrows}}$ ομοπαραλληλικές πολλαπλότητες του $k^n$ (γεωμετρικά αντικείμενα). Τώρα αν το $k$ είναι αλγεβρικά κλειστό, το Nullstellansatz (Hilbert, 1893) μας πληροφορεί ότι $I(V(J)) = \operatorname{rad} J$, όπου $\operatorname{rad} J = \{ f \in k[x_1,...,x_n] \mid f^m \in J \text{ για κάποιο } m \geq 1 \}$. Κατά συνέπεια, οι αντιστοιχίες

$$\text{ριζικά ιδεώδη του } k[x_1,...,x_n] \underset{J}{\overset{V}{\rightleftarrows}} \text{ομο/κές πολ/τες του } k^n$$

είναι αντίστροφες και $1-1$. (Ενα ιδεώδες $J$ λέγεται ριζικό αν $\operatorname{rad} J = J$). Δημιουργείται έτσι μια αμφίδρομη γέφυρα –διαφορετικού χαρακτήρα από το

πρόγραμμα Erlangen– με τη βοήθεια της οποίας η μελέτη γεωμετρικών ιδιοτήτων ομοπαραλληλικών πολλαπλοτήτων ανάγεται στη μελέτη Μεταθετικής Άλγεβρας (Κεφάλαιο 8).

*iii) Θεωρία Αναλλοιώτων*

Το κεντρικό πρόβλημα της θεωρίας αναλλοιώτων μπορεί να περιγραφεί ως εξής. Έστω $G$ μια ομάδα που δρα ως ομάδα αυτομορφισμών στο δακτύλιο $S = k[x_1,...,x_n]$. Ποια στοιχεία του $k[x_1,...,x_n]$ παραμένουν αναλλοίωτα κάτω από τη δράση; Το σύνολο των αναλλοιώτων $S^G = \{s \in S \mid gs = s \text{ για κάθε } g \in G\}$ είναι μια υποάλγεβρα της $S$. Αληθεύει ότι είναι πεπερασμένα παραγόμενη; ($14^{ο}$ πρόβλημα του Hilbert). Αν ναι, ποιο είναι ένα συγκεκριμένο πεπερασμένο σύνολο γεννητόρων; ($1^{ο}$ θεμελιώδες πρόβλημα της θεωρίας αναλλοιώτων).

Ο Hilbert (1890 και 1893) σε δύο καταπληκτικές εργασίες απέδειξε ότι η απάντηση στο $14^{ο}$ πρόβλημα είναι καταφατική για μια ευρεία κλάση περιπτώσεων. Το αποφασιστικό βήμα στις αποδείξεις του ήταν αυτό που σήμερα ονομάζεται *θεώρημα βάσης του Hilbert:* Κάθε ιδεώδες του δακτυλίου $k[x_1,...,x_n]$ ($k$ σώμα) και του $\mathbb{Z}[x_1,...,x_n]$ είναι πεπερασμένα παραγόμενο. Αργότερα η E. Noether αναγνώρισε ότι η κρίσιμη ιδιότητα των $k[x_1,...,x_n]$ και $\mathbb{Z}[x_1,...,x_n]$, απ' όπου έπεται το θεώρημα βάσης του Hilbert, είναι η συνθήκη αύξουσας ακολουθίας ιδεωδών. Έτσι φθάνουμε στη σύγχρονη διατύπωση του θεωρήματος του Hilbert: $R$ δακτύλιος της Noether $\Rightarrow R[x]$ δακτύλιος της Noether (Κεφάλαιο 4, § 7.4).

Ευχαριστώ θερμά την κα Π. Μπολιώτη για την επιμελημένη δακτυλογράφηση.

Μιχάλης Π. Μαλιάκας

# Κεφάλαιο 0

# Μεταθετικοί Δακτύλιοι, Ιδεώδη

Το κεφάλαιο αυτό έχει προπαρασκευαστικό χαρακτήρα. Θα καθιερώσουμε συμβολισμούς και θα υπενθυμίσουμε ορισμούς και στοιχειώδεις προτάσεις για δακτύλιους και ιδεώδη που είναι γνωστά από το μάθημα Βασική Άλγεβρα. Θα περιοριστούμε στα πλέον απαραίτητα για την ύλη που ακολουθεί.

## 0.1 Συμβολισμοί

Με $\mathbb{Z} = \{..., -1, 0, 1, ...\}$ και $\mathbb{N} = \{0, 1, ...\}$ συμβολίζουμε το σύνολο των ακεραίων αριθμών και το σύνολο των μη αρνητικών ακεραίων αριθμών αντίστοιχα. Το σύνολο των ρητών αριθμών είναι $\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$, το σύνολο των πραγματικών αριθμών συμβολίζεται με $\mathbb{R}$, ενώ το σύνολο των μιγαδικών αριθμών είναι $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, όπου $i^2 = -1$. Για σύνολα $A$ και $B$, χρησιμοποιούμε το συμβολισμό $A \subseteq B$ για να δηλώσουμε ότι το $A$ είναι υποσύνολο του $B$, ενώ ο συμβολισμός $A \underset{\neq}{\subseteq} B$ σημαίνει ότι το $A$ είναι γνήσιο υποσύνολο του $B$, δηλαδή $A \subseteq B$ και $A \neq B$. Ο πληθικός αριθμός ενός πεπερασμένου συνόλου $A$ συμβολίζεται με $\#A$. Αν $f : A \to B$ είναι συνάρτηση, $C \subseteq A$ και $D \subseteq B$ γράφουμε $f(C) = \{ f(c) \mid c \in C \}$ και $f^{-1}(D) = \{ a \in A \mid f(a) \in D \}$.

## 0.2 Δακτύλιοι, Παραδείγματα

*Δακτύλιος* είναι ένα μη κενό σύνολο $R$ εφοδιασμένο με δύο εσωτερικές πράξεις, πρόσθεση $+ : R \times R \to R$ και πολλαπλασιασμός $\cdot : R \times R \to R$ τέτοιες ώστε: α) το $R$ ως προς την πρόσθεση είναι αβελιανή ομάδα, β) ισχύουν

$r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$, $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$, $(r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$ για κάθε $r_1, r_2, r_3 \in R$, και γ) υπάρχει στοιχείο $1_R \in R$ έτσι ώστε $1_R \cdot r = r = r \cdot 1_R$ για κάθε $r \in R$.

Ένας δακτύλιος $R$ καλείται *μεταθετικός* αν ισχύει $r_1 \cdot r_2 = r_2 \cdot r_1$ για κάθε $r_1, r_2 \in R$.

Εφεξής θα γράφουμε $r_1 r_2$ στη θέση του $r_1 \cdot r_2$.

Επειδή στις σημειώσεις αυτές θα ασχοληθούμε αποκλειστικά με μεταθετικούς δακτυλίους, όταν *γράφουμε "δακτύλιο" θα εννοούμε μεταθετικό δακτύλιο*. Έτσι για παράδειγμα η φράση "έστω $R$ δακτύλιος" σημαίνει έστω $R$ μεταθετικός δακτύλιος.

Τα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ με τις συνήθεις πράξεις είναι δακτύλιοι. Το σύνολο των "ακεραίων του Gauss" $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ είναι επίσης δακτύλιος με τις συνήθεις πράξεις. Το σύνολο των κλάσεων υπολοίπων modulo $n$ $(n \in \mathbb{N})$, $\mathbb{Z}_n = \{[0],[1],...,[n-1]\}$, είναι δακτύλιος με πράξεις $[a] + [b] = [a + b]$ και $[a][b] = [ab]$ όπως θυμόσαστε από το μάθημα Βασική Άλγεβρα.

**0.2.1 Παράδειγμα** (*Τυπικές δυναμοσειρές*) Έστω $R$ ένας δακτύλιος. Θεωρούμε το σύνολο $R^{\mathbb{N}}$ των άπειρων ακολουθιών $(r_i)_{i \in \mathbb{N}} = (r_0, r_1, ..., r_n, ...)$ όπου $r_i \in R$ για κάθε $i \in \mathbb{N}$. Ορίζουμε την πρόσθεση και τον πολλαπλασιασμό

$$(r_i)_{i \in \mathbb{N}} + (s_j)_{j \in \mathbb{N}} = (r_i + s_i)_{i \in \mathbb{N}}$$

$$(r_i)_{i \in \mathbb{N}} (s_j)_{j \in \mathbb{N}} = (t_k)_{k \in \mathbb{N}},$$

όπου

$$t_k = r_0 s_k + r_1 s_{k-1} + \cdots + r_k s_0 = \sum_{i=0}^{k} r_i s_{k-i}$$

για κάθε $k \in \mathbb{N}$. Ως προς αυτές τις πράξεις το $R^{\mathbb{N}}$ είναι δακτύλιος με $1_{R^{\mathbb{N}}} = (1_R, 0_R, ...)$ και $0_{R^{\mathbb{N}}} = (0_R, 0_R, ...)$, όπου $0_R$ είναι το μηδενικό στοιχείο του $R$. Συνήθως συμβολίζουμε το στοιχείο $(r_i)_{i \in \mathbb{N}} = (r_0, r_1, ...)$ με

$$\sum_{i=0}^{\infty} r_i x^i = r_0 + r_1 x + \cdots,$$

οπότε οι πράξεις λαμβάνουν τη γνωστή μορφή

$$\sum_{i=0}^{\infty} r_i x^i + \sum_{i=0}^{\infty} s_j x^j = \sum_{i=0}^{\infty} (r_i + s_i) x^i$$
$$\left( \sum_{i=0}^{\infty} r_i x^i \right) \left( \sum_{j=0}^{\infty} s_j x^j \right) = \sum_{k=0}^{\infty} t_k x^k ,$$

όπου $t_k = r_0 s_k + r_1 s_{k-1} + \cdots + r_k s_0$. Με αυτόν το συμβολισμό γράφουμε $R[[x]] = R^{\mathbb{N}}$, και τα στοιχεία του δακτυλίου $R[[x]]$ ονομάζονται *τυπικές δυναμοσειρές*. Το σύνολο των τυπικών δυναμοσειρών $\sum_{i=0}^{\infty} r_i x^i$, όπου όλα τα $r_i$ εκτός από ένα πεπερασμένο πλήθος είναι ίσα με το $0_R$ είναι το σύνολο $R[x]$ των πολυωνύμων με συντελεστές από το *R*.

Ένα υποσύνολο *S* ενός δακτυλίου *R* ονομάζεται *υποδακτύλιος* του *R* αν το *S* είναι δακτύλιος ως προς τις ίδες πράξεις και $1_S = 1_R$. Από το προηγούμενο παράδειγμα, ο $R[x]$ είναι υποδακτύλιος του $R[[x]]$ για κάθε δακτύλιο *R*.

**0.2.2 Πρόταση** *Έστω S υποσύνολο του δακτυλίου R. Τότε ο S είναι υποδακτύλιος του R αν και μόνον αν*

*(i)* $1_R \in S$

*(ii)* $a, b \in S \Rightarrow a - b \in S$ *και* $ab \in S$.

**Απόδειξη.** Άσκηση □

Έστω *R* δακτύλιος. Η τομή (οποιουδήποτε πλήθους) υποδακτυλίων του *R* είναι υποδακτύλιος του *R*, πράγμα που προκύπτει άμεσα από την προηγούμενη πρόταση. Αν τώρα *A* είναι ένα μη κενό υποσύνολο του *R*, και *S* υποδακτύλιος του *R*, με $S[A]$ συμβολίζουμε την τομή όλων των υποδακτυλίων του *R* που περιέχουν το *S* και *A*. Αν το *A* είναι πεπερασμένο, $A = \{a_1, ..., a_n\}$, ο δακτύλιος $S[A]$ συμβολίζεται και με $S[a_1, ..., a_n]$. Με $S[x_1, ..., x_n]$ συμβολίζουμε το δακτύλιο των πολυωνύμων στις μεταβλητές $x_1, ..., x_n$ επί του *S*.

**0.2.2 Πρόταση** *Έστω ένας $R$ δακτύλιος και $S$ ένας υποδακτύλιος του $S$. Έστω $\{a_1,...,a_n\} \subseteq R$. Τότε*

$$S[a_1,...,a_n] = \{ f(a_1,...,a_n) \in R \mid f(x_1,...,x_n) \in S[x_1,...,x_n] \}.$$

**Απόδειξη.** Από την Πρόταση 0.2.2, το σύνολο $\{ f(a_1,...,a_n) \in R \mid f(x_1,...,x_n) \in S[x_1,...,x_n] \}$ είναι υποδακτύλιος του $R$. Επιπλέον περιέχει το σύνολο $\{a_1,...,a_n\}$. Άρα από τον ορισμό έχουμε $S[a_1,...,a_n] \subseteq \{ f(a_1,...,a_n) \in R \mid f(x_1,...,x_n) \in R[x_1,...,x_n] \}$. Για την άλλη σχέση εγκλεισμού παρατηρούμε ότι ο $\{ f(a_1,...,a_n) \in R \mid f(x_1,...,x_n) \in S[x_1,...,x_n] \}$ περιέχεται σε κάθε υποδακτύλιο του $R$ που περιέχει το $S$ και το $\{a_1,...,a_n\}$. Άρα ισχύει η ισότητα. □

Η προηγούμενη πρόταση εξηγεί το συμβολισμό $\mathbb{Z}[i]$ για τους ακέραιους του Gauss.

## 0.3 Ομομορφισμοί Δακτυλίων, Ιδεώδη

Έστω $R$ και $S$ δυο δακτύλιοι και $\varphi : R \to S$ μια απεικόνιση. Η $\varphi$ καλείται *ομομορφισμός δακτυλίων* αν

(i) $\varphi(r_i + r_2) = \varphi(r_1) + \varphi(r_2)$ για κάθε $r_1, r_2 \in R$

(ii) $\varphi(r_1 r_2) = \varphi(r_1) + \varphi(r_2)$ για κάθε $r_1, r_2 \in R$, και

(iii) $\varphi(1_R) = 1_S$.

Ένας ομομορφισμός δακτυλίων $\varphi : R \to S$ καλείται *επιμορφισμός* ή *μονομορφισμός* αν η $\varphi$ ως απεικόνιση είναι αντίστοιχα επί ή $1-1$. *Ισομορφισμός* είναι ομομορφισμός που είναι ταυτόχρονα επιμορφισμός και μονομορφισμός. Αν $\varphi : R \to S$ είναι ένας ισομορφισμός θα λέμε ότι οι δακτύλιοι $R$ και $S$ είναι *ισόμορφοι* και θα συμβολίζουμε αυτό με $R \cong S$. Για παράδειγμα, η απεικόνιση $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(m) = [m]$, είναι επιμορφισμός.

Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων. Το σύνολο $\ker\varphi = \{ r \in R \mid \varphi(r) = 0_S \}$ ονομάζεται *πυρήνας* του $\varphi$. Η *εικόνα* του $\varphi$ είναι $\mathrm{Im}\varphi = \{ s \in S \mid s = \varphi(r) \text{ για κάποιο } r \in R \}$. Χρησιμοποιώντας την Πρόταση 0.2.2

εύκολα αποδεικνύεται ότι το $\mathrm{Im}\varphi$ είναι υποδακτύλιος του $S$ (άσκηση). Επιπλέον έχουμε:

**0.3.1 Πρόταση** *Έστω* $\varphi: R \to S$ *ένας ομομορφισμός δακτυλίων. Τότε*

*(i)* *ο* $\varphi$ *είναι μονομορφισμός* $\Leftrightarrow \ker\varphi = \{0\}$.

*(ii)* *ο* $\varphi$ *είναι επιμορφισμός* $\Leftrightarrow \mathrm{Im}\varphi = S$.

**Απόδειξη.** (i) Έστω $\varphi$ μονομορφισμός. Αν $r \in \ker\varphi$ τότε $\varphi(r) = 0$ και άρα $\varphi(r) = \varphi(0_R)$. Όμως ο $\varphi$ είναι μονομορφισμός σημαίνει $r = 0_R$. Αντίστροφα έστω $\ker\varphi = \{0_R\}$. Αν $\varphi(r_1) = \varphi(r_2)$ με $r_1, r_2 \in R$, τότε $\varphi(r_1 - r_2) = 0_S$ και άρα $r_1 - r_2 \in \ker\varphi$. Συνεπώς $r_1 = r_2$.

(ii) Προφανές από τους ορισμούς. □

Έστω $R$ ένας δακτύλιος και $I$ ένα μη κενό υποσύνολο του $R$. Το $I$ καλείται *ιδεώδες* του $R$ αν i) $a + b \in I$ για κάθε $a, b \in I$ και ii) $ra \in I$ για κάθε $r \in R$ και $a \in I$. Για παράδειγμα, αν $\varphi: R \to S$ είναι ένας ομομορφισμός δακτυλίων, τότε ο πυρήνας $\ker\varphi$ είναι ιδεώδες του $R$ (άσκηση). Ένα ιδεώδες $I$ του $R$ λέγεται *γνήσιο* αν $I \neq R$.

Ένα ιδεώδες του δακτυλίου $R$ λέγεται *κύριο* αν έχει τη μορφή $I = \{ra \mid r \in R\}$ για κάποιο $a \in I$. Στην περίπτωση αυτή θα γράφουμε $I = (a)$ και θα λέμε ότι το $I$ *παράγεται* από το $a$.

Έστω $A$ ένα υποσύνολο του δακτυλίου $R$. Το *ιδεώδες που παράγεται από το* $A$ είναι το ιδεώδες

$$\left\{ \sum_{i=1}^{m} r_i a_i \in R \mid m = 1,2,..., r_i \in R, a_i \in A \quad \text{για κάθε} \quad i = 1,2,...,m \right\}$$

και το συμβολίζουμε $(A)$. Αν το $A$ είναι πεπερασμένο $A = \{a_1,...,a_n\}$ χρησιμοποιούμε και το συμβολισμό $(a_1,...,a_n)$ στη θέση του $(A)$.

Έστω $I$ ένα ιδεώδες του δακτυλίου $R$. Το σύνολο των πλευρικών κλάσεων $R/I = \{r + I \mid r \in R\}$ έχει τη δομή δακτυλίου με τις πράξεις $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$, $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Πράγματι, το μόνο πράγμα που δεν είναι τελείως προφανές είναι ότι οι προηγούμενες πράξεις είναι καλά ορισμένες: έστω

$r_1 + I = r_1' + I$ και $r_2 + I = r_2' + I$. Τότε έχουμε $r_1 - r_1' \in I$ και $r_2 - r_2' \in I$. Για την πρόσθεση παρατηρούμε ότι $(r_1 + r_2) - (r_1' + r_2') = (r_1 - r_1') + (r_2 - r_2') \in I$ και άρα $(r_1 + r_2) + I = (r_1' + r_2') + I$. Για τον πολλαπλασιασμό παρατηρούμε ότι $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$ και άρα $r_1 r_2 + I = r_1' r_2' + I$. Ο $R/I$ καλείται *δακτύλιος πηλίκο*.

Είδαμε ότι σε κάθε μονορφισμό δακτυλίων $\varphi : R \to S$ αντιστοιχεί ο πυρήνας $\ker\varphi$ που είναι ιδεώδες του *R*. Αντίστροφα, έστω *I* ιδεώδες του *R*. Τότε ο ομομορφισμός δακτυλίων $\varphi : R \to R/I$, $f(r) = r + I$ (που καλείται *φυσικός επιμορφισμός*) έχει πυρήνα $\ker\varphi = I$. Έτσι υπάρχει στενή σχέση μεταξύ των εννοιών ομομορφισμός, ιδεώδες και δακτύλιος πηλίκο. Μία άλλη σχέση δίνεται από το παρακάτω αποτέλεσμα.

**0.3.2 Θεώρημα** (*Το $1^ο$ Θεώρημα Ισομορφισμών Δακτυλίων*) *Έστω* $\varphi : R \to S$ *ένας ομομορφισμός δακτυλίων. Τότε υπάρχει ισομορφισμός δακτυλίων*

$$\overline{\varphi} : R/\ker\varphi \to \mathrm{Im}\,\varphi, \quad \overline{\varphi}(r + \ker\varphi) = \varphi(r)\,.$$

**Απόδειξη.** Η $\overline{\varphi}$ είναι καλά ορισμένη. Πράγματι, αν $r + \ker\varphi = r' + \ker\varphi$, τότε $r - r' \in \ker\varphi$ και άρα $\varphi(r - r') = 0$. Δηλαδή $\varphi(r) = \varphi(r')$ και κατά συνέπεια $\overline{\varphi}(r + \ker\varphi) = \overline{\varphi}(r' + \ker\varphi)$. Το ότι ο $\overline{\varphi}$ είναι ομομορφισμός δακτυλίων βεβαιώνεται με έναν υπολογισμό ρουτίνας που παραλείπεται. Προφανώς ο $\overline{\varphi}$ είναι επί. Μένει να δείξουμε ότι είναι μονομορφισμός. Από την Πρόταση 0.3.1 (i) αρκεί να δείξουμε ότι $\ker\overline{\varphi} = \{0_{R/\ker\varphi}\}$. Πράγματι, παρατηρούμε ότι $\overline{\varphi}(r + \ker\varphi) = 0_S \Rightarrow \varphi(r) = 0_S \Rightarrow r \in \ker\varphi \Rightarrow r + \ker\varphi = \ker\varphi = 0_{R/\ker\varphi}$.

□

Η επόμενη πρόταση περιγράφει τα ιδεώδη του δακτυλίου πηλίκου $R/I$ και θα χρησιμοποιηθεί συχνά στα παρακάτω.

**0.3.3 Πρόταση** *Έστω I ένα ιδεώδες του δακτυλίου R. Κάθε ιδεώδες του* $R/I$ *έχει τη μορφή* $J/I$ *όπου J είναι ιδεώδες του R που περιέχει το I.*

**Απόδειξη.** Σημειώνουμε πρώτα μία γενική παρατήρηση: αν $\varphi : R \to S$ είναι ένας ομομορφισμός δακτυλίων και *K* ένα ιδεώδες του *S*, τότε η αντίστροφη εικόνα $\varphi^{-1}(K) = \{r \in R \mid \varphi(r) \in K\}$ είναι ένα ιδεώδες του *R*. Πράγματι, $r_1, r_2 \in \varphi^{-1}(K) \Rightarrow \varphi(r_1),\ \varphi(r_2) \in K \Rightarrow \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) \in K \Rightarrow r_1 + r_2 \in K$, και $a \in R,\ r \in \varphi^{-1}(I) \Rightarrow \varphi(ar) = \varphi(a)\varphi(r) \in K \Rightarrow ar \in \varphi^{-1}(K)$. Εφαρμόζουμε τώρα την προηγούμενη παρατήρηση στον φυσικό επιμορφισμό $f : R \to R/I$. Έστω *K* ένα ιδεώδες του $R/I$. Το $f^{-1}(K)$ είναι ιδεώδες του *R*, που προφανώς περιέχει το *I*, για το οποίο ισχύει $f^{-1}(K)/I = K$. □

## 0.4 Κατασκευή Νέων Ιδεωδών από Παλαιά

Από τον ορισμό του ιδεώδους προκύπτει άμεσα ότι η τομή μιας μη κενής οικογένειας ενός δακτυλίου είναι και πάλι ιδεώδες.

Όμως δεν συμβαίνει το ίδιο για την ένωση. Για παράδειγμα η ένωση $(2) \cup (3)$ των κύριων ιδεωδών (2) και (3) του $\mathbb{Z}$ δεν είναι ιδεώδες (γιατί;). Ένα υποκατάστατο της ένωσης ιδεωδών είναι η πράξη του αθροίσματος ιδεωδών: έστω $(I_\lambda)_{\lambda \in \Lambda}$ μια οικογένεια ιδεωδών του δακτυλίου *R*. Το *άθροισμα* των $I_\lambda$ είναι το ιδεώδες του *R* που παράγεται από το σύνολο $\bigcup_{\lambda \in \Lambda} I_\lambda$, δηλαδή είναι το ιδεώδες

$$\left( \bigcup_{\lambda \in \Lambda} I_\lambda \right) = \left\{ \sum_\lambda r_\lambda c_\lambda \mid r_\lambda \in R,\ c_\lambda \in I_\lambda, \text{ και } r_\lambda = 0 \right.$$

$$\left. \text{εκτός από ένα πεπερασμένο πλήθος } \lambda \right\}.$$

Το συμβολίζουμε με $\sum_{\lambda \in \Lambda} I_\lambda$. Στην ειδική περίπτωση που το $\Lambda$ είναι πεπερασμένο σύνολο, $\Lambda = \{1,2,...,n\}$ χρησιμοποιούμε συνήθως το συμβολισμό $\sum_{i=1}^{n} I_i$ ή και $I_1 + \cdots + I_n$ και παρατηρούμε ότι ισχύει

$$\sum_{i=1}^{n} I_i = \{c_1 + \cdots + c_n \mid c_i \in I_i \text{ για } i = 1,...,n\}.$$

**0.4.1 Παράδειγμα** *Έστω* $m,n \in \mathbb{N}$. *Τότε στο* $\mathbb{Z}$ *ισχύει* $(m)+(n)=(d)$, *όπου d είναι ο μέγιστος κοινός διαιρέτης των m και n.*

**Απόδειξη.** Εφόσον το $m$ είναι πολλαπλάσιο του $d$, έχουμε $(m) \subseteq (d)$. Όμοια $(n) \subseteq d$. Άρα από τον ορισμό $(m)+(n) \subseteq (d)$. Για την άλλη σχέση εγκλεισμού, γράφουμε το $d$ ως γραμμικό συνδυασμό των $m$ και $n$ (το $d$ είναι ο μέγιστος κοινός διαιρέτης των $m$ και $n$). Έχουμε $d = mx + ny$, όπου $x, y \in \mathbb{Z}$. Άρα από τον ορισμό $d \in (m)+(n)$, και κατά συνέπεια $(d) \subseteq (m)+(n)$. □

Μια άλλη χρήσιμη πράξη ιδεωδών είναι το γινόμενο. Έστω $I$ και $J$ ιδεώδη του $R$. Με $IJ$ συμβολίζουμε το ιδεώδες που παράγεται από το σύνολο $\{ab \in R \mid a \in I, b \in J\}$. Αυτό ονομάζεται *γινόμενο* των $I$ και $J$. Η προσεταιριστικότητα του γινομένου στο $R$ μας επιτρέπει να ορίσουμε κατά τον προφανή τρόπο το γινόμενο πεπερασμένου πλήθους ιδεωδών: Έστω $I_1,...,I_n$ ιδεώδη του $R$. Τότε ορίζουμε το ιδεώδες $\prod_{i=1}^{n} I_i = I_1 I_2 \cdots I_n$ ως το ιδεώδες του $R$ που παράγεται από το σύνολο $\{a_1 a_2 \cdots a_n \mid a_i \in I_i \text{ για } i = 1,2,...,n\}$. Παρατηρούμε ότι $\prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i$.

Μετά την τομή, το άθροισμα και το γινόμενο ολοκληρώνουμε την "αριθμητική" των ιδεωδών ορίζοντας το ιδεώδες πηλίκο: Έστω $I$ και $J$ ιδεώδη του $R$. Θέτουμε $(I:J) = \{r \in R \mid rJ \subseteq I\}$. Αυτό είναι ένα ιδεώδες του $R$ για το οποίο ισχύει $I \subseteq (I:J)$. Ονομάζεται *ιδεώδες πηλίκο*. Στην ειδική περίπτωση $I = (0)$, το ιδεώδες πηλίκο $(0:J) = \{r \in R \mid rJ = 0\} = \{r \in R \mid ra = 0 \text{ για κάθε } a \in J\}$ ονομάζεται *μηδενιστής του J* και συμβολίζεται με $\operatorname{Ann} J$.

## 0.5 Ακέραιες Περιοχές και Σώματα

Ένας δακτύλιος $R$ (μεταθετικός όπως πάντα!) ονομάζεται *ακέραια περιοχή* ή απλώς *περιοχή* αν $0_R \neq 1_R$ και η σχέση $ab = 0$ με $a \in R$ και $b \in R$ ισχύει μόνο αν

$a=0$ ή $b=0$. Για παράδειγμα οι δακτύλιοι $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Z}_3$ είναι περιοχές, ενώ ο $\mathbb{Z}_4$ δεν είναι.

**0.5.1 Πρόταση** *Ο δακτύλιος $\mathbb{Z}_n$ είναι περιοχή αν και μόνον αν ο n είναι πρώτος.*

**Απόδειξη.** Έστω *n* πρώτος. Αν $[a][b]=[0]$ στο $\mathbb{Z}_n$, τότε το *n* διαιρεί το γινόμενο $ab$. Εφόσον ο *n* είναι πρώτος, θα διαιρεί έναν τουλάχιστον από τους *a* και *b*. Άρα $[a]$ ή $[b]=0$, και συνεπώς ο $\mathbb{Z}_n$ είναι περιοχή.

Αντίστροφα, έστω ότι ο $\mathbb{Z}_n$ είναι περιοχή. Τότε αν $n=ab$ $(a,b\in N)$ με $1<a<n$ και $1<b<n$, έχουμε $[0]=[a][b]$ όπου $[a]\neq 0$ και $[b]\neq 0$. Αυτό είναι άτοπο. □

Ένας δακτύλιος $R$ λέγεται *σώμα* αν $0_R\neq 1_R$ και κάθε $a\in R-\{0\}$ είναι αντιστρέψιμο. Προφανώς κάθε σώμα είναι περιοχή.

**0.5.2 Πρόταση** *Κάθε πεπερασμένη περιοχή είναι σώμα.*

**Απόδειξη.** Έστω *R* πεπερασμένη περιοχή και $a\in R$ με $a\neq 0$. Θα δείξουμε ότι το *a* είναι αντιστρέψιμο. Έστω $R=\{a_1,a_2,...,a_n\}$. Θεωρούμε τα στοιχεία $aa_1,aa_2,...,aa_n$. Αυτά είναι διακεκριμένα μεταξύ τους· πράγματι αν $aa_i=aa_j$ τότε $a(a_i-a_j)=0$ και αφού $a\neq 0$ και *R* είναι περιοχή, έχουμε $a_i=a_j$. Το πλήθος τους είναι *n* και άρα κάποιο απ' αυτά θα είναι το στοιχείο $1_R$, δηλαδή $aa_i=1_R$ για κάποιο *i*. Άρα το *a* είναι αντιστρέψιμο. □

**0.5.3 Πόρισμα** *Ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα αν και μόνον αν ο n είναι πρώτος.*

**Απόδειξη.** Άμεση από τις Προτάσεις 0.5.1 και 0.5.2. □

**0.5.4 Ορισμός** *Έστω k σώμα. Μια k-άλγεβρα R είναι ένας δακτύλιος R εφοδιασμένος με μια απεικόνιση $k\times R\ni(a,r)\mapsto a\cdot r\in R$ που ικανοποιεί τις συνθήκες: Το R είναι k-διασματικός χώρος και*

$$a\cdot(r_1r_2)=(a\cdot r_1)r_2=r_1(a\cdot r_2)\quad \text{για κάθε}\quad a\in k,\ \ r_1,r_2\in R\,.$$

Για παράδειγμα, ο δακτύλιος $k[x]$ είναι μια $k$ άλγεβρα.

**0.5.5 Ορισμός** *Έστω $R$ και $S$ δύο $k$-άλγεβρες. Μια απεικόνιση $\varphi: R\to S$ ονομάζεται ομομορφισμός (αντίστοιχα, μονομορφισμός, επιμορφισμός, ισομορφισμός) αλγεβρών αν είναι ομομορφισμός (αντίστοιχα, μονομορφισμός, επιμορφισμός, ισομορφισμός) δακτυλίων και επιπλέον ισχύει*

$$\varphi(ar)=a\varphi(r)$$

*για κάθε $a\in k$ και $r\in R$.*

Για παράδειγμα, έστω $a\in k$. Η απεικόνιση ("εκτίμηση στο $a$")

$$k[x]\ni f(x)\mapsto f(a)\in k$$

είναι ένας επιμορφισμός $k$-αλγεβρών.

## 0.6 Πρώτα και Μέγιστα Ιδεώδη

Θυμίζουμε εδώ τα πλέον βασικά περί πρώτων και μέγιστων ιδεωδών.

**0.6.1 Ορισμός** *Ένα ιδεώδες $P$ του $R$ καλείται πρώτο αν*

*(i)* $P\neq R$, *και*

*(ii) αν* $a,b\in R$ *με* $ab\in P$ *τότε* $a\in P$ *ή* $b\in P$.

**0.6.2 Πρόταση** *Έστω $I$ ιδεώδες του $R$. Τότε το $I$ είναι πρώτο αν και μόνο αν ο δακτύλιος πηλίκο $R/I$ είναι περιοχή.*

**Απόδειξη.** Έστω $I$ πρώτο. Τότε $I\neq R$ και $R/I\neq 0$. Έστω $a,b\in R$ με την ιδιότητα $(a+I)(b+I)=0_{R/I}$. Τότε $ab+I=I$ και άρα $ab\in I$. Συνεπώς $a\in I$ ή $b\in I$ δηλαδή $a+I=0_{R/I}$ ή $b+I=0_{R/I}$.

Αντίστροφα, έστω $R/I$ ακέραια περιοχή. Τότε $R/I\neq 0$ και άρα $I\neq R$. Έστω $a,b\in R$ με $ab\in I$. Τότε $ab+I=0_{R/I}\Rightarrow (a+I)(b+I)=0_{R/I}\Rightarrow$ $a+I=0_{R/I}$ ή $b+I=0_{R/I}\Rightarrow a\in I$ ή $b\in I$. □

**0.6.3 Ορισμός** *Ένα ιδεώδες $M$ του $R$ ονομάζεται μέγιστο αν*

*(i)* $M \neq R$, *και*

*(ii) δεν υπάρχει ιδεώδες I του R με την ιδιότητα* $M \subsetneq I \subsetneq R$.

**0.6.4 Πρόταση** *Έστω I ένα ιδεώδες του R. Τότε το I είναι μέγιστο αν και μόνο αν ο δακτύλιος πηλίκο* $R/I$ *είναι σώμα.*

**Απόδειξη.** Έστω ότι το $I$ είναι μέγιστο. Τότε $I \neq R$ και $R/I \neq 0$. Έστω $a+I \in R/I$ με $a+I \neq 0_{R/I}$. Θα δείξουμε ότι το $a+I$ είναι αντιστρέψιμο. Εφόσον $a+I \neq 0_{R/I}$ ισχύει $a \notin I$. Το ιδεώδες $(a)+I$ περιέχει γνήσια το $I$. Αφού το $I$ είναι μέγιστο έχουμε $(a)+I = R$. Άρα για κάποια $r \in R$ και $b \in I$ ισχύει $ra+b=1$. Συνεπώς $(r+1)(a+I) = ra+I = (1-b)+I = 1+I$ και το $r+I$ είναι αντιστρέψιμο.

Αντίστροφα, έστω ότι ο $R/I$ είναι σώμα. Τότε $R/I \neq 0$ και άρα $I \neq R$. Έστω $J$ ιδεώδες με $I \subsetneq J \subsetneq R$. Θα δείξουμε ότι $J = R$, οπότε το $I$ είναι μέγιστο. Υπάρχει $a \in J$, $a \notin I$. Άρα $a+I \neq 0_{R/I}$ και, αφού το $R/I$ είναι σώμα, $(a+I)(b+I) = 1+I$ για κάποιο $b \in R$. Άρα

$$ab-1 \in I.$$

Εφόσον $I \subseteq J$ και $a \in J$ συμπεραίνουμε ότι $1 \in J$, δηλαδή $J = R$. □

**0.6.5 Πόρισμα** *Κάθε μέγιστο ιδεώδες είναι πρώτο.*

**Απόδειξη.** Άμεση από τις Προτάσεις 0.6.4 και 0.6.2. □

Για παράδειγμα, το ιδεώδες $(x)$ του $\mathbb{Z}[x]$ είναι πρώτο, γιατί $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ που είναι περιοχή, και όχι μέγιστο αφού ο $\mathbb{Z}$ δεν είναι σώμα. Το ιδεώδες $(2,x)$ του $\mathbb{Z}[x]$ είναι μέγιστο, αφού $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}_2$ (γιατί;) που είναι σώμα. Στο επόμενο κεφάλαιο θα περιγράψουμε όλα τα πρώτα (και μέγιστα) ιδεώδη του $\mathbb{Z}[x]$ (Πρόταση 1.4.1).

## 0.7 Σώμα Πηλίκων Ακέραιας Περιοχής

Θυμίζουμε εδώ την κατασκευή του σώματος πηλίκων μιας ακέραιες περιοχής *R*. Ειδικότερα θα δούμε πως ο *R* εμφυτεύεται ως υποδακτύλιος σ' ένα σώμα σε αναλογία με την εμφύτευση του $\mathbb{Z}$ στο $\mathbb{Q}$.

**0.7.1 Πρόταση** *Έστω R μια περιοχή. Τότε υπάρχει σώμα k και μονομορφισμός δακτυλίων* $\varphi : R \to k$ *έτσι ώστε κάθε στοιχείο του k γράφεται στη μορφή* $\varphi(r)\varphi(s)^{-1}$ *για κάποια* $r, s \in R$, $s \neq 0$.

**Απόδειξη.** Θέτουμε $S = R - \{0\}$. Στο σύνολο $R \times S$ ορίζουμε μια σχέση ισοδυναμίας

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc .$$

Η κλάση ισοδυναμίας που περιέχει το στοιχείο $(a,b)$ συμβολίζεται $\frac{a}{b}$. Το σύνολο των κλάσεων ισοδυναμίας, έστω *k*, είναι σώμα με πράξεις

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{B}\frac{c}{d} = \frac{ac}{bd}$$

(Η επαλήθευση του καλώς ορισμένου των πράξεων και των αξιωμάτων είναι θέμα ρουτίνας και παραλείπεται). Το μηδέν του σώματος αυτού είναι το $\frac{0}{1}$ και το μοναδιαίο στοιχείο είναι το $\frac{1}{1}$. Τέλος η συνάρτηση $\varphi : R \to k$, $\varphi(a) = \frac{a}{1}$ για κάθε $a \in R$, είναι μονομορφισμός δακτυλίων και το τυχαίο $\frac{a}{b} \in k$ γράφεται $\varphi(a)\varphi(b)^{-1}$.

□

Το σώμα που κατασκευάσαμε πιο πάνω ονομάζεται *σώμα πηλίκων* του *R*. Για παράδειγμα, το σώμα πηλίκων του $\mathbb{Z}$ είναι το $\mathbb{Q}$ και το σώμα πηλίκων του $k[x]$ (*k* σώμα) είναι το σώμα των ρητών συναρτήσεων

$$k(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], g(x) \neq 0 \right\}.$$

## 0.8 Επεκτάσεις Σωμάτων

Αν $E \supseteq F$ είναι σώματα (ως προς τις ίδιες πράξεις) θα λέμε ότι το $E$ είναι *επέκταση* του $F$. Συμβολικά γράφουμε $E/F$. Ο *βαθμός* της επέκτασης $E/F$ είναι η διάσταση του $E$ ως $F$-διανυσματικός χώρος. Συμβολικά $[E:F] = \dim_F E$. Μια επέκταση σωμάτων $E/F$ λέγεται πεπερασμένη αν $[E:F] < \infty$. Ένα στοιχείο $a \in E$ λέγεται *αλγεβρικό* επί του $F$ αν είναι ρίζα κάποιου μη μηδενικού πολυωνύμου $f(x) \in F[x]$. Για παράδειγμα το $\sqrt{2} \in \mathbb{R}$ είναι αλγεβρικό επί του $\mathbb{Q}$, γιατί είναι ρίζα του $x^2 - 2 \in \mathbb{Q}[x]$. Μια επέκταση $E/F$ λέγεται αλγεβρική αν κάθε $a \in E$ είναι αλγεβρικό επί του $F$.

**0.8.1 Πρόταση** *Κάθε πεπερασμένη επέκταση σωμάτων είναι αλγεβρική.*

**Απόδειξη.** Έστω $E/F$ επέκταση με $[E:F] = n < \infty$. Έστω $a \in E$. Τα στοιχεία

$$1 = a^0, a^1, a^2, ..., a^n$$

είναι γραμμικώς εξαρτημένα επί του $F$ γιατί το πλήθος τους είναι $n+1 > n$. Άρα υπάρχουν $\lambda_0, \lambda_1, ..., \lambda_n \in F$ (όχι όλα μηδέν) με την ιδιότητα

$$\lambda_0 + \lambda_1 a + \cdots + \lambda_n a^n = 0.$$

Αν θέσουμε

$$f(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n \in F[x]$$

τότε $f(x) \neq 0$ και το $a$ είναι ρίζα του $f(x)$. □

Ένα σώμα $F$ λέγεται *αλγεβρικά κλειστό* αν κάθε μη σταθερό πολυώνυμο $f(x) \in F[x]$ έχει μια τουλάχιστον ρίζα στο $F$. Συνεπώς ένα σώμα $F$ είναι αλγεβρικά κλειστό αν κάθε μη σταθερό πολυώνυμο $f(x) \in F[x]$ γράφεται ως γινόμενο πρωτοβάθμιων παραγόντων στο $F[x]$.

Αναφέρουμε χωρίς απόδειξη ότι για κάθε σώμα $F$ υπάρχει επέκταση $\overline{F}/F$ όπου το $\overline{F}$ είναι αλγεβρικά κλειστό σώμα. Το $\overline{F}$ είναι μοναδικό (με προσέγγιση ισομορφισμού) και ονομάζεται *αλγεβρική θήκη* του $F$. Για παράδειγμα η αλγεβρική θήκη του $\mathbb{R}$ είναι το $\mathbb{C}$, πράγμα που έπεται από το Θεμελιώδες Θεώρημα της Άλγεβρας, που παραθέτουμε χωρίς απόδειξη.

**0.8.2 Θεμελιώδες Θεώρημα της Άλγεβρας** *Το σώμα $\mathbb{C}$ είναι αλγεβρικά κλειστό.*

**0.8.3 Θεώρημα** *Αν οι επεκτάσεις σωμάτων* $E/F$ *και* $K/E$ *είναι πεπερασμένες, τότε η επέκταση* $K/F$ *είναι πεπερασμένη και*

$$[K:F]=[K:E][E:F].$$

**Απόδειξη.** Έστω $[E:F]=n$ και $[K:E]=m$. Έστω

$$a_1,...,a_n$$

μια βάση του $E$ ως $F$-διανυσματικός χώρος και

$$b_1,...,b_m$$

μια βάση του $K$ ως $E$-διανυσματικός χώρος. Θα δείξουμε ότι το σύνολο

$$X=\{a_ib_j\in K \mid i=1,...,n,\ j=1,...,m\}$$

αποτελεί μία βάση του $K$ ως $F$-διανυσματικός χώρος.

Έστω $c\in K$. Τότε το $c$ είναι $E$-γραμμικός συνδυασμός των στοιχείων $b_1,...,b_m$. Επειδή κάθε στοιχείο του $E$ είναι $F$-γραμμικός συνδυασμός των στοιχείων $a_1,...,a_n$ συμπεραίνουμε ότι το $c$ είναι $F$-γραμμικός συνδυασμός των στοιχείων $a_ib_j$. Άρα το $X$ παράγει το $K$ επί του $F$.

Έστω

$$\sum_{i,j}\lambda_{ij}a_ib_j=0 \quad (\lambda_{ij}\in F).$$

Γράφοντας

$$\sum_{i,j}\lambda_{ij}a_ib_j=\sum_j\left(\sum_i\lambda_{ij}a_i\right)b_j=0$$

συμπεραίνουμε ότι

$$\sum_i\lambda_{ij}a_i=0$$

γιατί τα $b_j$ αποτελούν βάση. Η τελευταία σχέση δίνει $\lambda_{ij}=0$, γιατί τα $a_i$ αποτελούν βάση. Συνεπώς το $X$ είναι γραμμικά ανεξάρτητο επί του $F$. □

## 0.9 Θεμελιώδες Θεώρημα Συμμετρικών Πολυωνύμων

Ένα πολυώνυμο $f(x_1,...,x_n)\in R[x_1,...,x_n]$ ονομάζεται *συμμετρικό* αν για κάθε μετάθεση $\sigma$ των στοιχείων $1,2,...,n$ ισχύει

$$f(x_{\sigma(1)},...,x_{\sigma(n)})=f(x_1,...,x_n).$$

Για παράδειγμα, τα ακόλουθα πολυώνυμα είναι συμμετρικά

$$e_1 = x_1 + x_2 + \cdots + x_n$$
$$e_2 = x_1x_2 + \cdots + x_1x_n + \cdots + x_{n-1}x_n$$
$$\cdots$$
$$e_n = x_1x_2 \cdots x_n .$$

Τα $e_i$ ονομάζονται *στοιχειώδη* συμμετρικά πολυώνυμα. Παρατηρούμε ότι αυτά εμφανίζονται ως συντελεστές (με προσέγγιση προσήμου) του πολυωνύμου $(x-x_1)(x-x_2)\cdots(x-x_n) \in R[x_1,...,x_n][x]$ αφού

$$(x-x_1)\cdots(x-x_n) = x^n - e_1x^{n-1} + e_2x^{n-2} - \cdots + (-1)^n e_n .$$

**0.9.1 Θεμελιώδες Θεώρημα Συμμετρικών Πολυωνύμων** *Κάθε συμμετρικό πολυώνυμο είναι πολυώνυμο στα στοιχειώδη συμμετρικά πολυώνυμα.*

Δηλαδή αν $f(x_1,...,x_n)$ είναι ένα συμμετρικό πολυώνυμο, τότε ισχύει $f(x_1,...,x_n) = g(e_1,...,e_n)$ για κάποιο $g(x_1,...,x_n) \in R[x_1,...,x_n]$. Για παράδειγμα $x_1^2 + \cdots + x_n^2 = e_1^2 - 2e_2$.

**Απόδειξη.** Θα δώσουμε μια στοιχειώδη απόδειξη που είναι μάλιστα κατασκευαστική.

Ορίζουμε μια ολική διάταξη στα μονώνυμα $x_1^{a_1} \cdots x_n^{a_n}$

$$x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n}$$

αν η πρώτη μη μηδενική διαφορά $a_i - b_i$ είναι θετική. (Η διάταξη αυτή συνήθως καλείται *λεξικογραφική*). Για παράδειγμα $x_1^2x_2 > x_1x_2^2 > x_1x_2$.

Έστω $f(x_1,...,x_n)$ ένα συμμετρικό πολυώνυμο και

$$x_1^{a_1} \cdots x_n^{a_n}$$

το μέγιστο μονώνυμο του $f(x_1,...,x_n)$ ως προς τη λεξικογραφική διάταξη. Επειδή το $f(x_1,...,x_n)$ είναι συμμετρικό θα περιέχει κάθε μονώνυμο που λαμβάνεται από το $x_1^{a_1} \cdots x_n^{a_n}$ με κάποια μετάθεση των $a_1,...,a_n$. Συνεπώς ισχύει

$$a_1 \geq a_2 \geq \cdots \geq a_n .$$

Θεωρούμε τώρα το μέγιστο μονώνυμο που περιέχεται στο πολυώνυμο

$$e_1^{a_1}\cdots e_n^{a_n}.$$

Το μονώνυμο αυτό είναι το

$$x_1^{a_1+\cdots+a_n}x_2^{a_2+\cdots+a_n}\cdots x_n^{a_n}.$$

Συνεπώς το μέγιστο μονώνυμο που περιέχει το πολυώνυμο

$$e_1^{a_1-a_2}e_2^{a_2-a_3}\cdots e_n^{a_n}$$

είναι το

$$x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}.$$

Έστω $c$ ο συντελεστής του $x_1^{a_1}\cdots x_n^{a_n}$ στο $f(x_1,...,x_n)$. Τότε το μέγιστο μονώνυμο του πολυωνύμου

$$f_1 = f(x_1,...,x_n) - ce_1^{a_1-a_2}e_2^{a_2-a_3}\cdots e_n^{a_n}$$

είναι μικρότερο από το $x_1^{a_1}\cdots x_n^{a_n}$. Έχουμε $\deg f_1 \le \deg f(x_1,...,x_n)$ γιατί $\deg e_1^{a_1-a_2}e_2^{a_2-a_3}\cdots e_n^{a_n} = a_1+\cdots+a_n$. Επαναλαμβάνουμε τη διαδικασία στο $f_1$, κοκ. Όμως το πλήθος των μονωνύμων που είναι μικρότερα του $x_1^{a_1}\cdots x_n^{a_n}$ και έχουν βαθμό $\le \deg f(x_1,...,x_n)$ είναι βέβαια πεπερασμένο. Έτσι, μετά ένα πεπερασμένο πλήθος βήματα, έχουμε $f_k = 0$, δηλαδή το $f(x_1,...,x_n)$ γράφεται ως πολυώνυμο στα $e_1,...,e_n$. □

Για παράδειγμα, έστω $n=3$ και

$$f(x_1,x_2,x_3) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2.$$

Τότε

$$a_1 = 2,\quad a_2 = 1,\quad a_3 = 0,$$

και

$$f_1 = f(x_1,x_2,x_3) - e_1e_2,$$

σύμφωνα με την απόδειξη. Όμως με πράξεις διαπιστώνουμε ότι $f(x_1,x_2,x_3) - e_1e_2 = -3x_1x_2x_3$. Άρα

$$f(x_1,x_2,x_3) = e_1e_2 - 3e_3.$$ □

## Ασκήσεις

**1*.** Ο δακτύλιος $R$ είναι ακέραια περιοχή αν και μόνο αν ο δακτύλιος $R[x]$ είναι ακέραια περιοχή.

**2.** Το στοιχείο $\sum_{i=0}^{\infty} r_i x^i \in R[[x]]$ είναι αντιστρέψιμο αν και μόνο αν το στοιχείο $r_0 \in R$ είναι αντιστρέψιμο.

**3.** Δώστε ένα παράδειγμα ενός υποδακτυλίου του $\mathbb{Q}[x]$ που δεν είναι ιδεώδες του $\mathbb{Q}[x]$.

**4.** Αποδείξτε ότι το ιδεώδες $(2, x)$ του $\mathbb{Z}[x]$ δεν είναι κύριο.

**5.** Για τα κύρια ιδεώδη $I = (m)$, $I = (n)$ του $\mathbb{Z}$ ποια είναι τα ιδεώδη $I \cap J$, $I + J$, $IJ$ και $(I : J)$; Η απάντηση να δοθεί συναρτήσει της παραγοντοποίησης των $m$ και $n$ σε γινόμενα πρώτων αριθμών.

**6*.** Έστω $I, J, K$ ιδεώδη του $R$, και έστω $(I_\lambda)_{\lambda \in \Lambda}$ μια οικογένεια ιδεωδών του $R$. Αποδείξτε τις παρακάτω σχέσεις.

(i) $\big((I : J) : K\big) = (I : JK) = \big((I : K) : J\big)$

(ii) $\left(\bigcap_{\lambda \in \Lambda} I_\lambda : K\right) = \bigcap_{\lambda \in \Lambda} (I_\lambda : K)$

(iii) $\left(J : \sum_{\lambda \in \Lambda} I_\lambda\right) = \bigcap_{\lambda \in \Lambda} (J : I_\lambda)$

**7.** Στον δακτύλιο $\mathbb{Q}[x_1, x_2, x_3, x_4]$ θεωρούμε τα ιδεώδη $I = (x_1, x_2)$ και $J = (x_3, x_4)$. Αποδείξτε ότι $IJ \neq \{fg \mid f \in I,\ g \in J\}$.

**8.** Έστω $I, J, K$ ιδεώδη του δακτυλίου $R$.

(i) Ισχύει ότι $IJ = I \cap J$;

(ii) Αποδείξτε ότι $I \cap (J + K) \supseteq I \cap J + I \cap K$;

(iii) Αν $I + J = R$ αποδείξετε ότι $IJ = I \cap J$.

**9.** Είναι ισόμορφοι οι δακτύλιοι $\mathbb{Z}[i]$ και $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$;

**10.** Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων όπου το $S$ είναι περιοχή. Αποδείξτε ότι το ιδεώδες $\ker \varphi$ είναι πρώτο.

**11.** Κάθε περιοχή με πεπερασμένο πλήθος ιδεωδών είναι σώμα.

**12.** Έστω $R$ ένας πεπερασμένος δακτύλιος. Τότε κάθε πρώτο ιδεώδες του $R$ είναι μέγιστο.

**13.** Ο δακτύλιος $\mathbb{Z}[x]$ έχει άπειρο πλήθος μέγιστων ιδεωδών.

**14*.** Σωστό (απαιτείται απόδειξη) ή Λάθος (αρκεί ένα αντιπαράδειγμα). Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων

(i) $I$ ιδεώδες του $R \Rightarrow \varphi(I)$ ιδεώδες του $S$.

(ii) $I$ ιδεώδες του $R$ και $\varphi$ επιμορφισμός $\Rightarrow \varphi(I)$ ιδεώδες του $S$.

(iii) $J$ ιδεώδες του $S \Rightarrow \varphi^{-1}(J)$ ιδεώδες του $R$.

(iv) $P$ πρώτο ιδεώδες του $R$, $\varphi$ επιμορφισμός $\Rightarrow \varphi(P)$ πρώτο ιδεώδες του $S$.

(v) $P$ πρώτο ιδεώδες του $R$, $\varphi$ επιμορφισμός, $\ker\varphi \subseteq P \Rightarrow \varphi(P)$ πρώτο ιδεώδες του $S$.

(vi) $M$ μέγιστο ιδεώδες του $R$, $\varphi$ επιμορφισμός, $\ker\varphi \subseteq M \Rightarrow \varphi(M)$ μέγιστο ιδεώδες του $S$.

**15.** Έστω $I \subseteq J$ ιδεώδη του $R$. Τότε υπάρχει ισομορφισμός

$$(R/I)/(J/I) \to R/J$$
$$(r+I)+J/I \mapsto r+J$$

(Υπόδειξη: Εφαρμόστε το Θεώρημα 0.3.2).

**16*.** Έστω $I \subseteq J$ ιδεώδη του $R$. Τότε

(a) Το ιδεώδες $J/I$ του $R/I$ είναι πρώτο $\Leftrightarrow$ το $J$ είναι πρώτο

(b) Το ιδεώδες $J/I$ του $R/I$ είναι μεγιστο $\Leftrightarrow$ το $J$ είναι μέγιστο.

(Υπόδειξη: Άσκηση 15).

**17*.** (Ταυτότητα διαίρεσης) Έστω $f, g \in R[x]$. Αν ο μεγιστοβάθμιος συντελεστής του $g(x)$ είναι αντιστρέψιμο στοιχείο του $R$, τότε υπάρχουν $q, r \in R[x]$ με τις ιδιότητες

(1) $f = qg + r$

(2) $\deg r < \deg q$

Επιπλέον, τα $q$, $r$ είναι μοναδικά.

(Υπόδειξη: για την ύπαρξη, χρησιμοποιήσετε επαγωγή στο $m = \deg f$. Για το επαγωγικό βήμα, παρατηρήσετε ότι ο βαθμός του $f - a_m b_n^{-1} x^{m-n} g$, όπου $f = a_m x^m + \cdots + a_0$ και $g = b_n x^n + \cdots + b_0$ είναι $< m$).

**18*.** (Κριτήριο του Eisenstein). Έστω $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ και $p \in \mathbb{Z}$ πρώτος αριθμός. Αν

(i) $p$ διαιρεί τους $a_0, a_1, ..., a_{n-1}$

(ii) $p$ δεν διαιρεί τον $a_n$

(iii) $p^2$ δεν διαιρεί τον $a_0$

τότε το $f$ είναι ανάγωγο πολυώνυμο στο $\mathbb{Z}[x]$.

(Παρατήρηση: ισχύει το ισχυρότερο συμπέρασμα ότι το $f$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Βλέπε Λήμμα 1.3.4 στο επόμενο Κεφάλαιο).

**19.** Εφαρμόστε το θεμελιώδες θεώρημα των συμμετρικών πολυωνύμων στο πολυώνυμο $x_1^4 + x_2^4 + x_1^3 x_2 + x_1 x_2^3$ $(n = 2)$.

**20.** Αποδείξτε ότι το $\mathbb{Q}[\sqrt{2}]$ είναι ισόμορφο με το σώμα πηλίκων του $\mathbb{Z}[\sqrt{2}]$.

**21.** Στην απόδειξη της Πρότασης 0.7.1, που χρησιμοποιήθηκε η υπόθεση ότι το $R$ είναι ακέραια περιοχή;

# Κεφάλαιο 1

# Παραγοντοποίηση σε Ακέραιες Περιοχές

Γνωρίζουμε ότι στο $\mathbb{Z}$ κάθε στοιχείο εκτός από το 0 και τα $\pm 1$ γράφεται ως γινόμενο πρώτων αριθμών κατά τρόπο ουσιαστικά μοναδικό. Από τη Βασική Άλγεβρα ξέρουμε ότι κάτι ανάλογο συμβαίνει στο δακτύλιο πολυωνύμων $k[x]$, όπου $k$ είναι σώμα. Σκοπός μας εδώ είναι να μελετήσουμε ακέραιες περιοχές που έχουν την ιδιότητα της "μοναδικής παραγοντοποίησης". Για να γίνουμε πιο σαφείς απαιτούνται μερικοί ορισμοί που παραθέτουμε αμέσως παρακάτω.

## 1.1 Ορισμοί και Παραδείγματα

Έστω $R$ ένας δακτύλιος και $a, b \in R$.

**1.1.1 Ορισμός** *i) Θα λέμε ότι το $a$ διαιρεί το $b$ (συμβολισμός $a \mid b$) αν υπάρχει $c \in R$ τέτοιο ώστε $b = ac$.*

*ii) Τα $a$ και $b$ ονομάζονται συντροφικά στο $R$ αν $a = ub$ για κάποιο αντιστρέψιμο $u \in R$.*

Η σχέση στο $R$ που ορίζεται από $a \sim b \Leftrightarrow a$ και $b$ είναι συντροφικά, είναι σχέση ισοδυναμίας.

Για παράδειγμα, τα μόνα συντροφικά στοιχεία του 3 στο $\mathbb{Z}$ είναι το 3 και $-3$. Τα συντροφικά στοιχεία του $f(x) \in k[x]$, όπου $k$ είναι σώμα, είναι τα $uf(x)$ όπου $u \in k - \{0\}$.

**1.1.2 Ορισμός** *Έστω $R$ μια ακέραια περιοχή και $p \in R$. Τότε το $p$ ονομάζεται ανάγωγο στο $R$ αν*

*(i) το $p$ δεν είναι μηδέν και δεν είναι αντιστρέψιμο, και*

*(ii) $p = ab$ με $a, b \in R$ ισχύει μόνο αν το $a$ ή το $b$ είναι αντιστρέψιμο.*

Προφανώς οι πρώτοι αριθμοί είναι ανάγωγοι στο $\mathbb{Z}$. Όμως ο πρώτος αριθμός 5 δεν είναι ανάγωγο στοιχείο στο $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ αφού $5=(1+2i)(1-2i)$ και τα στοιχεία $1+2i$, $1-2i$ δεν είναι αντιστρέψιμα στο $\mathbb{Z}[i]$. (Απόδειξη: $(1+2i)(m+ni)=1\Rightarrow m-2n=1$ και $2m+n=0$ το οποίο δεν έχει ακέραιες λύσεις. Όμοια για το $1-2i$. Δες την Πρόταση 1.5.4 παρακάτω).

**1.1.3 Ορισμός** *Μια ακέραια περιοχή R ονομάζεται περιοχή μοναδικής παραγοντοποίησης αν ισχύουν οι παρακάτω συνθήκες:*

*(i) Κάθε στοιχείο του R που δεν είναι 0 ή αντιστρέψιμο γράφεται ως γινόμενο αναγώγων στοιχείων στο R.*

*(ii) Αν $a=p_1\cdots p_r$ και $a=q_1\cdots q_s$ είναι γινόμενα αναγώγων στοιχείων του R τότε $r=s$ και μετά από κάποια αρίθμηση, το $p_i$ είναι συντροφικό του $q_i$ για κάθε $i=1,...,r$.*

Γνωστά παραδείγματα είναι οι δακτύλιοι $\mathbb{Z}$ και $k[x]$, όπου $k$ σώμα. Ένα άλλο παράδειγμα είναι ο δακτύλιος $R[x_1,...,x_n]$ των πολυωνύμων πολλών μεταβλητων με συντελεστές από μία ακέραια περιοχή $R$, όπως θα δείξουμε αργότερα στο κεφάλαιο αυτό. Ο $\mathbb{Z}[i]$ είναι επίσης περιοχή μοναδικής παραγοντοποίησης όπως θα δούμε παρακάτω. Υπάρχουν πολλές περιοχές που δεν είναι περιοχές μοναδικής παραγοντοποίησης. Ένα τέτοιο παράδειγμα είναι το επόμενο.

**1.1.4 Παράδειγμα** Θα δείξουμε ότι στην ακέραια περιοχή $\mathbb{Z}[\sqrt{-5}]=\{a+b\sqrt{-5} \mid a,b\in\mathbb{Z}\}$ δεν ισχύει η συνθήκη (ii) του Ορισμού 1.1.3. Παρατηρούμε ότι

$$6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5}).$$

Πρώτα δείχνουμε ότι τα στοιχεία 2, 3, $1+\sqrt{-5}$, και $1-\sqrt{-5}$ είναι ανάγωγα στο $\mathbb{Z}[\sqrt{-5}]$: Ορίζουμε μία συνάρτηση (“νόρμα”)

$$N:\mathbb{Z}[\sqrt{-5}]\ni a+b\sqrt{-5}\mapsto a^2+5b^2\in\mathbb{N}$$

και παρατηρούμε ότι $N(xy)=N(x)N(y)$ για κάθε $x,y\in\mathbb{Z}[\sqrt{-5}]$. Έστω τώρα ότι το $u\in\mathbb{Z}[\sqrt{-5}]$ είναι αντιστρέψιμο. Από τη σχέση $uv=1$ παίρνουμε $N(uv)=N(1)=1$, δηλαδή $N(u)N(v)=1$. Άρα $N(u)=1$, γιατί $N(u),N(v)\in\mathbb{N}$. Γράφοντας $u=u_0+u_1\sqrt{-5}$, παίρνουμε $u_0^2+5u_1^2=1$ ($u_0,u_1\in\mathbb{Z}$). Οι λύσεις της τελευταίας Διοφαντικής εξίσωσης είναι προφανώς $u_0=\pm1$, $u_1=0$. Συμπέρασμα: τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{-5}]$ είναι τα $\pm1$. Επομένως τα 2, 3, $1\pm\sqrt{-5}$ δεν είναι αντιστρέψιμα (συνθήκη i) του Ορισμού 1.1.2). Θα δείξουμε τώρα ότι ισχύει η συνθήκη ii) του Ορισμού 1.1.2 για καθένα από τα 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$. Έστω $2=ab$ με $a,b\in\mathbb{Z}[\sqrt{-5}]$. Έχουμε $N(2)=N(ab)$, δηλαδή $4=N(a)N(b)$. Επειδή $N(a),N(b)\in\mathbb{N}$, συμπεραίνουμε ότι $N(a)=1$ ή $N(a)=2$ ή $N(a)=4$. Η περίπτωση $N(a)=1$ αποκλείεται γιατί $N(a)=1\Rightarrow a=\pm1$. Όμοια η περίπτωση $N(a)=4$ αποκλείεται γιατί $N(a)=4\Rightarrow N(b)=1\Rightarrow b=\pm1$. Άρα έχουμε $N(a)=2$. Όμως γράφοντας $a_0+a_1\sqrt{-5}$ με $a_0,a_1\in\mathbb{Z}$ παρατηρούμε ότι $N(a)=2\Leftrightarrow a_0^2+5a_1^2=2$. Η τελευταία Διοφαντική εξίσωση δεν έχει λύσεις. Συνεπώς το 2 είναι ανάγωγο στο $\mathbb{Z}[\sqrt{-5}]$. Με παρόμοιο τρόπο δείχνουμε ότι το 3, $1+\sqrt{-5}$, και $1-\sqrt{-5}$ είναι ανάγωγα στο $\mathbb{Z}[\sqrt{-5}]$. Τέλος είναι προφανές ότι από τα 2, 3, $1+\sqrt{-5}$, και $1-\sqrt{-5}$ οποιαδήποτε δύο δεν είναι συντροφικά, γιατί τα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{-5}]$ είναι τα $\pm1$.

Υπενθυμίζουμε ότι ένα ιδεώδες $I$ του δακτυλίου $R$ ονομάζεται κύριο αν $I=(a)$ για κάποιο $a\in R$ (§ 0.3).

**1.1.5 Ορισμός** *Μια περιοχή R ονομάζεται περιοχή κυρίων ιδεωδών αν κάθε ιδεώδες του R είναι κύριο.*

**1.1.6 Παράδειγμα** Οι δακτύλιοι $\mathbb{Z}$ και $k[x]$, όπου $k$ είναι σώμα, είναι περιοχές κυρίων ιδεωδών.

**Απόδειξη.** Έστω $I$ ιδεώδες του $\mathbb{Z}$ διάφορο από το $(0)$. Έστω $d \in I$ ο ελάχιστος μη μηδενικός φυσικός αριθμός του συνόλου $I \cap \mathbb{N}$. Θα αποδείξουμε ότι $I = (d)$. Προφανώς $(d) \subseteq I$. Έστω λοιπόν $m \in I$. Από την ταυτότητα διαίρεσης στο $\mathbb{Z}$ έχουμε

$$m = qd + r, \qquad 0 \le r < d .$$

Συνεπώς $r = m - qd \in I$, γιατί το $I$ είναι ιδεώδες. Από την ανισότητα $0 \le r < d$ και τον ορισμό του $d$ συμπεραίνουμε ότι $r = 0$. Τελικά $m = qd \in (d)$, δηλαδή $I \subseteq (d)$. Η απόδειξη για το $k[x]$ είναι πανομοιότυπη: χρησιμοποιήστε την ταυτότητα διαίρεσης πολυωνύμων. (Άσκηση 0.17).

Ένα παράδειγμα περιοχής που δεν είναι περιοχή κυρίων ιδεωδών επισημάνθηκε ήδη στην Άσκηση 0.4. Ένα άλλο τέτοιο παράδειγμα είναι ο δακτύλιος $k[x, y]$ των πολυωνύμων δύο μεταβλητών πάνω στο σώμα $k$ (γιατί;).

Έχοντας λοιπόν κατανοήσει τους προηγούμενους ορισμούς, μπορούμε να περιγράψουμε το στόχο αυτού του Κεφαλαίου, ο οποίος είναι να αποδείξουμε ότι:

**1.** Κάθε περιοχή κυρίων ιδεωδών είναι περιοχή μοναδικής παραγοντοποίησης (1.2.1 Θεώρημα).

**2.** $R$ περιοχή μοναδικής παραγοντοποίησης $\Rightarrow R[x]$ είναι περιοχή μοναδικής παραγοντοποίησης (1.3.1 Θεώρημα).

## 1.2 Κύρια Ιδεώδη και Παραγοντοποίηση

Θα αποδείξουμε εδώ το ακόλουθο

**1.2.1 Θεώρημα** *Κάθε περιοχή κυρίων ιδεών είναι περιοχή μοναδικής παραγοντοποίησης.*

Το πρώτο βήμα στην απόδειξη του παραπάνω θεωρήματος είναι να δείξουμε ότι σε κάθε περιοχή κυρίων ιδεωδών κάθε μη μηδενικό, μη αντιστρέψιμο στοιχείο γράφεται ως γινόμενο αναγώγων στοιχείων (1.2.3 Πρόταση παρακάτω). Για το σκοπό αυτό χρειαζόμαστε το ακόλουθο λήμμα.

**1.2.2 Λήμμα** *Έστω R μια περιοχή κυρίων ιδεωδών και έστω*

$$I_1 \subseteq I_2 \subseteq \cdots$$

*μια αύξουσα ακολουθία ιδεωδών του R. Τότε υπάρχει* $m \in \mathbb{N}$ *τέτοιο ώστε*

$$I_m = I_{m+1} = I_{m+2} = \cdots .$$

**Απόδειξη.** Θεωρούμε την ένωση $I = \bigcup_{i=1}^{\infty} I_i$. Θα δείξουμε ότι το *I* είναι ιδεώδες του *R*. Πράγματι, έστω $a, b \in I$ και $r \in R$. Για κάποια *i* και *j* έχουμε $a \in I_i$, και $b \in I_j$ λόγω της υπόθεσης. Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $i \le j$. Τότε $a, b \in I_j$. Κατά συνέπεια $a + b \in I_j$ και $ra \in I_j$. Άρα $a + b \in I$ και $ra \in I$. Συνεπώς το *I* είναι ιδεώδες. Τώρα, επειδή ο *R* είναι περιοχή κυρίων ιδεωδών, έχουμε $I = (c)$ για κάποιο $c \in I$. Όμως αφού $I = \bigcup_{i=1}^{\infty} I_i$, έχουμε $c \in I_m$ για κάποιο *m*. Άρα για κάθε $n \ge m$ έχουμε $I_m = I_n$.

□

**1.2.3 Πρόταση** *Έστω R μια περιοχή κυρίων ιδεωδών. Τότε κάθε μη μηδενικό, μη αντιστρέψιμο στοιχείο του R είναι γινόμενο αναγώγων στοιχείων του R.*

**Απόδειξη.** Έστω $a \in R$ με $a \neq 0$ και *a* μη αντιστρέψιμο. Πρώτα θα αποδείξουμε ότι υπάρχει ανάγωγο $p \in R$ που διαιρεί το *a*. Αν το *a* είναι ανάγωγο, δεν υπάρχει τίποτε να αποδείξουμε. Έστω ότι το *a* δεν είναι ανάγωγο. Τότε υπάρχουν μη αντιστρέψιμα στοιχεία $a_1, b_1 \in R$ με την ιδιότητα $a = a_1 b_1$. Αυτό σημαίνει ότι

$$(a) \subsetneq (a_1) .$$

Πράγματι $a = a_1 b_1 \Rightarrow (a) \subseteq (a_1)$. Αν $(a) = (a_1)$ τότε $a = x a_1$ και $a_1 = ya$ για κάποια $x, y \in R$. Τότε $a = yab = ayb_1 \Rightarrow a(1 - yb_1) = 0 \Rightarrow 1 - yb_1 = 0 \Rightarrow b_1$ αντιστρέψιμο, που είναι άτοπο. Επαναλαμβάνουμε την προηγούμενη διαδικασία για το $a_1$ στη θέση του *a* κοκ. Λαμβάνουμε λοιπόν μια γνησίως αύξουσα ακολουθία ιδεωδών του *R*

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots .$$

Από το Λήμμα 1.2.2, η παραπάνω ακολουθία τερματίζει σε κάποιο $(a_m)$. Το $p = a_m$ είναι ανάγωγο εξ ορισμού και διαιρεί το *a*.

Έχουμε αποδείξει ότι είτε το $a$ είναι ανάγωγο είτε $a = p_1 c_1$, όπου $p_1$ ανάγωγο και $c_1$ μη αντιστρέψιμο. Στη δεύτερη περίπτωση έχουμε

$$(a) \subsetneq (c_1)$$

όπως και πριν. Αν το $c_1$ είναι ανάγωγο, δεν υπάρχει τίποτε να αποδείξουμε. Έστω ότι το $c_1$ δεν είναι ανάγωγο. Τότε $c_1 = p_2 c_2$ για κάποιο ανάγωγο $p_2$ και μη αντιστρέψιμο $c_2$. Επαναλαμβάνοντας τη διαδικασία λαμβάνουμε μια γνησίως αύξουσα ακολουθία ιδεωδών του $R$

$$(a) \subsetneq (c_1) \subsetneq (c_2) \subsetneq \cdots.$$

Από το Λήμμα 1.2.2, αυτή κάπου τερματίζει, έστω στο $(c_m)$. Τότε το $c_m$ είναι ανάγωγο και ισχύει $a = p_1 p_2 \cdots p_m c_m$. □

Το δεύτερο βήμα στην απόδειξη του Θεωρήματος 1.2.1 είναι να δείξουμε τη μοναδικότητα της παραγοντοποίησης που παρέχει η Πρόταση 1.2.3. Χρειαζόμαστε για περιοχές κυρίων ιδεωδών μια πρόταση ανάλογη με την ακόλουθη πρόταση για το $\mathbb{Z}$: αν ο πρώτος $p$ διαιρεί το γινόμενο $ab$, τότε θα διαιρεί έναν τουλάχιστον από τα $a$ και $b$. Αυτή η πρόταση είναι το κύριο βήμα στην απόδειξη της μοναδικότητας της παραγοντοποίησης στο $\mathbb{Z}$.

**1.2.4 Λήμμα** *Έστω $R$ περιοχή κυρίων ιδεωδών και $p \notin R$. Τότε το $p$ είναι ανάγωγο αν και μόνο αν το ιδεώδες $(p)$ είναι μέγιστο.*

**Απόδειξη.** Έστω $(p)$ μέγιστο ιδεώδες. Έστω $p = ab$ με $a, b \in R$. Θα δείξουμε ότι το $a$ ή το $b$ είναι αντιστρέψιμο. Έχουμε $(p) \subseteq (a)$. Από τον ορισμό του μεγίστου ιδεώδους έχουμε $(a) = (p)$ ή $(a) = R$. Στην πρώτη περίπτωση ισχύει $p = au$ για κάποιο αντιστρέψιμο $u$, πράγμα που σημαίνει ότι $b = a$ είναι αντιστρέψιμο. Στη δεύτερη περίπτωση το $a$ είναι αντιστρέψιμο.

Αντίστροφα, έστω ότι το $p$ είναι ανάγωγο. Έστω $I$ ιδεώδες του $R$ με την ιδιότητα $(p) \subseteq I$. Επειδή ο $R$ είναι δακτύλιος κυρίων ιδεωδών έχουμε $I = (a)$ για κάποιο $a \in R$. Άρα $p = ab$ για κάποιο $b \in R$. Αν το $a$ είναι αντιστρέψιμο, έχουμε

$(a) = R$. Αν όχι, τότε το $b$ είναι αντιστρέψιμο γιατί το $p$ είναι ανάγωγο, οπότε ισχύει $(a) = (p)$. Αποδείξαμε ότι $I = R$ ή $I = (p)$. Άρα το $(p)$ είναι μέγιστο. □

**1.2.5 Πρόταση** *Έστω $R$ μια περιοχή κυρίων ιδεωδών και $p \in R$ ανάγωγο. Αν $p \mid ab$, όπου $a, b \in R$, τότε $p \mid a$ ή $p \mid b$.*

**Απόδειξη.** Έχουμε $p \mid ab \Rightarrow (ab) \in (p)$. Από το Λήμμα 1.2.4 το ιδεώδες $(p)$ είναι μέγιστο και κατά συνέπεια (Πόρισμα 0.6.5) πρώτο. Άρα $a \in (p)$ ή $b \in (p)$. □

Με επαγωγή αποδείχνεται αμέσως το παρακάτω πόρισμα.

**1.2.6 Πόρισμα** *Έστω $R$ μια περιοχή κυρίων ιδεωδών και $p \in R$ ανάγωγο. Αν $p \mid a_1 \cdots a_n$, όπου $a_1, ..., a_n \in R$, τότε για κάποιο $i$ έχουμε $p \mid a_i$.* □

Έχοντας υπόψη το προηγούμενο πόρισμα, η απόδειξη του δεύτερου βήματος είναι απλούστατη:

**Απόδειξη του Θεωρήματος 1.2.1.** Από την Πρόταση 1.2.3 αρκεί να δείξουμε τη συνθήκη (ii) του Ορισμού 1.1.3. Έστω λοιπόν $a = p_1 \cdots p_r$ και $a = q_1 \cdots q_s$ γινόμενα αναγώγων στοιχείων του $R$ με $s \geq r$. Από τη σχέση $p_1 \cdots p_r = q_1 \cdots q_s$ και το Πόρισμα 1.2.6 συμπεραίνουμε ότι το $p_1$ διαιρεί κάποιο $q_j$. Μετά από κάποια αρίθμηση μπορούμε να υποθέσουμε ότι $p_1 \mid q_1$. Άρα $q_1 = u_1 p_1$ για κάποιο αντιστρέψιμο $u_1$, γιατί το $q_1$ είναι ανάγωγο. Άρα $p_1 \cdots p_r = u_1 p_1 q_2 \cdots q_s$ και αφού ο $R$ είναι ακέραια περιοχή,

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s .$$

Συνεχίζοντας κατά αυτόν τον τρόπο καταλήγουμε σε μια σχέση της μορφής

$$1 = u_1 \cdots u_r q_{r+1} \cdots q_s .$$

Επειδή τα $q_{r+1}, ..., q_s$ είναι ανάγωγα και άρα μη αντιστρέψιμα θα ισχύει $r = s$. □

Αναφέρουμε εδώ ότι το αντίστροφο του Θεωρήματος 1.2.1 δεν ισχύει: ο δακτύλιος $k[x, y]$ είναι περιοχή μοναδικής παραγοντοποίησης (δες το Πόρισμα 1.3.5 παρακάτω) αλλά όχι περιοχή κυρίων ιδεωδών.

Από το Θεώρημα 1.2.1 και το Παράδειγμα 1.1.6 λαμβάνουμε και πάλι το ακόλουθο αποτέλεσμα.

**1.2.6 Πόρισμα** *Οι δακτύλιοι* $\mathbb{Z}$ *και* $k[x]$ *(k σώμα) είναι ακέραιες περιοχές μοναδικής παραγοντοποίησης.*

Αμέσως παρακάτω θα γενικεύσουμε το προηγούμενο πόρισμα όπου στη θέση του σώματος $k$ θα έχουμε τυχαία περιοχή μοναδικής παραγοντοποίησης.

## 1.3 Περιοχές Μοναδικής Παραγοντοποίησης και Πολυώνυμα

**1.3.1 Θεώρημα** *Αν ο δακτύλιος R είναι περιοχή μοναδικής παραγοντοποίησης τότε και ο* $R[x]$ *είναι περιοχή μοναδικής παραγοντοποίησης.*

Θα δώσουμε εδώ την κλασσική απόδειξη που οφείλεται ουσιαστικά στον Gauss. Έχει το πλεονέκτημα ότι τα κύρια βήματα είναι "διαισθητικά προφανή". Η κεντρική ιδέα είναι η ακόλουθη: έστω $R$ μια περιοχή μοναδικής παραγοντοποίησης και $f(x) \in R[x]$. Θεωρούμε το σώμα πηλίκων του $R$, έστω $k$, και την παραγοντοποίηση του $f(x) \in k[x]$ σύμφωνα με το Πόρισμα 1.2.6. Συγκρίνοντας τα ανάγωγα στοιχεία του $R[x]$ με τα ανάγωγα στοιχεία του $k[x]$ λαμβάνουμε την παραγοντοποίηση του $f(x) \in R[x]$.

Αν $a_0, a_1, ..., a_n$ είναι στοιχεία –όχι όλα μηδέν– μιας ακέραιας περιοχής μπορούμε να θεωρήσουμε στοιχεία $d$ έτσι ώστε $d \mid a_0, d \mid a_1, ..., d \mid a_n$. Κάθε τέτοιο $d$ ονομάζεται κοινός διαιρέτης των $a_0, a_1, ..., a_n$. Αν τώρα $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ είναι ένα μη μηδενικό πολυώνυμο, $f(x) \in R[x]$ όπου $R$ ακεραία περιοχή, με την ιδιότητα κάθε κοινός διαιρέτης των $a_0, a_1, ..., a_n$ είναι αντιστρέψιμο στοιχείο του $R$, τότε αυτό ονομάζεται *πρωταρχικό πολυώνυμο*. Για

παράδειγμα το $2x^2+3x-4\in\mathbb{Z}[x]$ είναι πρωταρχικό, ενώ το $2x^2+2x-4\in\mathbb{Z}[x]$ δεν είναι.

Έστω $a,b\in R-\{0\}$ δύο στοιχεία της περιοχής μοναδικής παραγοντοποίησης $R$. Αν $a=up_1^{a_1}\cdots p_k^{a_k}$ και $b=vp_1^{b_1}\cdots p_k^{b_k}$ είναι αναλύσεις σε γινόμενα αναγώγων στοιχείων, όπου $u$ και $v$ είναι αντιστρέψιμα στοιχεία, τα $p_i$ δεν είναι συντροφικά ανά δύο, και $a_i,b_i\in\mathbb{N}$, τότε κάθε στοιχείο της μορφής $c=wp_1^{c_1}\cdots p_k^{c_k}$, όπου $w$ αντιστρέψιμο στοιχείο του $R$ και $c_i=\min\{a_i,b_i\}$ ονομάζεται *μέγιστος κοινός διαιρέτης* (μ.κ.δ.) των $a,b$. Η έννοια του μ.κ.δ. δεν ορίζεται μονοσήμαντα: αν $c$ είναι μ.κ.δ. των $a$ και $b$, τότε και το $uc$ είναι μ.κ.δ. των $a$ και $b$ για κάθε αντιστέψιμο $u$. Όταν γράφουμε μ.κ.δ. $(a,b)=c$ θα εννοούμε ότι κάθε $uc$ είναι ένας μ.κ.δ. των $a,b$. Αν τώρα $f(x)\in R[x]$ με $f(x)\neq 0$ είναι φανερό ότι $f(x)=cg(x)$, όπου $c$ είναι ένας μ.κ.δ. των συντελεστών του $f(x)$ και $g(x)\in R[x]$ είναι πρωταρχικό. Κάθε τέτοιο $c$ ονομάζεται *περιεχόμενο* του $f(x)$. Για παράδειγμα, $6x^2-12x+4=2(3x^2-6x+2)$ αλλά και $6x^2-12x+4=(-2)(-3x^2+6x-2)$, οπότε ένα περιεχόμενο του $6x^2-12x+4$ είναι το 2 και ένα άλλο είναι το $-2$. Το παρακάτω προφανές λήμμα μας δίνει μια μορφή μοναδικότητας των $c$ και $g(x)$.

**1.3.2 Λήμμα** *Έστω $f(x)\in R[x]$ ένα μη σταθερό πολυώνυμο, όπου $R$ περιοχή μοναδικής παραγοντοποίησης. Έστω $f(x)=cg(x)$ και $f(x)=c'g'(x)$, όπου $c$, $c'$ είναι περιεχόμενα του $f(x)$ και $g(x)$, $g'(x)$ είναι πρωταρχικά πολυώνυμα. Τότε υπάρχουν αντιστρέψιμα $u,v\in R$ έτσι ώστε $c=uc'$ και $g(x)=vg'(x)$.*

**Απόδειξη.** Η σχέση $c=uc'$ προκύπτει άμεσα από τον ορισμό του περιεχομένου. Για τη δεύτερη σχέση παρατηρούμε ότι $cg(x)=c'g'(x)\Rightarrow uc'g(x)=c'g'(x)\Rightarrow ug(x)=g'(x)$. □

**1.3.3 Λήμμα** *(Gauss) Έστω $R$ μια περιοχή μοναδικής παραγοντοποίησης. Τότε το γινόμενο δύο πρωταρχικών πολυωνύμων στο $R[x]$ είναι πρωταρχικό.*

**Απόδειξη.** Έστω $f(x), g(x) \in R[x]$ πρωταρχικά. Έστω ότι το γινόμενο $f(x)\ g(x)$ δεν είναι πρωταρχικό. Τότε υπάρχει ανάγωγο $p \in R$ που διαιρεί όλους τους συντελεστές του $f(x)\ g(x)$. Θεωρούμε τον επιμορφισμό δακτυλίων

$$\varphi : R[x] \to R/(p)[x]$$

$$a_0 + \cdots + a_n x^n \mapsto \overline{a}_0 + \cdots + \overline{a}_n x^n$$

όπου $\overline{a}_i = a_i + (p) \in R/(p)$.

Έχουμε $\varphi(f(x)g(x)) = 0$ και άρα $\varphi(f(x))\varphi(g(x)) = 0$. Όμως το ιδεώδες $(p)$ είναι πρώτο αφού το $p$ είναι ανάγωγο $(ab \in (p) \Rightarrow p \mid ab \Rightarrow p \mid a$ ή $p \mid b$ αφού $R$ περιοχή μονοσήμαντης ανάλυσης $\Rightarrow a \in (p)$ ή $b \in (p))$. Άρα το $R/(p)$ είναι περιοχή (Πρόταση 0.6.2). Συνεπώς ο $R/(p)[x]$ είναι ακέραια περιοχή (Άσκηση 0.1). Άρα $\varphi(f(x)) = 0$ ή $\varphi(g(x)) = 0$. Αυτό σημαίνει ότι το $p$ θα διαιρεί όλους τους συντελεστές είτε του $f(x)$ είτε του $g(x)$, πράγμα άτοπο. □

**1.3.4 Λήμμα** *Έστω R μια περιοχή μοναδικής παραγοντοποίησης και k το σώμα πηλίκων του R. Έστω $f(x) \in R[x]$ ένα μη σταθερό πολυώνυμο.*

*(i) Αν το $f(x)$ είναι ανάγωγο στο $R[x]$, τότε είναι ανάγωγο και στο $k[x]$*

*(ii) Αν το $f(x)$ είναι ανάγωγο στο $k[x]$ και πρωταρχικό στο $R[x]$, τότε είναι ανάγωγο και στο $R[x]$.*

**Απόδειξη.** (i) Έστω $f(x) = g(x)h(x)$ με $g(x).h(x) \in k[x]$. Το $k$ είναι το σώμα πηλίκων του $R$. Άρα, απαλείφοντας τους παρονομαστές των συντελεστών των $g(x)$ και $h(x)$, έχουμε

$$df(x) = g_1(x)h_1(x),$$

όπου $d \in R$, $g_1(x) \in R[x]$ $\deg g_1(x) = \deg g(x)$ και $\deg h_1(x) = \deg h(x)$. Γράφουμε $f(x) = cf_1(x)$, $g_1(x) = c_1 g_2(x)$, και $h_1(x) = c_2 h_2(x)$ για πρωταρχικά πολυώνυμα $f_1(x), g_2(x), h_2(x) \in R[x]$ και $c_1, c_2, c_3 \in R$ (δες την παράγραφο πριν το Λήμμα 1.3.2). Έχουμε

$$dcf_1(x) = c_1 c_2 g_2(x) h_1(x)$$

και από το Λήμμα 1.3.3, το $g_2(x)h_2(x)$ είναι πρωταρχικό. Από το Λήμμα 1.3.2 έχουμε $c_1c_2 = dcu$ για κάποιο αντιστρέψιμο $u \in R$. Συνεπώς

$$dcf_1(x) = dcug_2(x)h_2(x).$$

Άρα $f(x) = cf_1(x) = cug_2(x)h_2(x)$. Συμπέρασμα: $f(x) = g(x)h(x)$ στο $F[x]$ συνεπάγεται $f(x) = cug_2(x)h_2(x)$ στο $R[x]$ με $\deg g_2(x) = \deg g(x)$ και . Άρα $f(x)$ ανάγωγο στο $R[x] \Rightarrow f(x)$ ανάγωγο στο $k[x]$.

(ii) Προφανές αφού $R[x] \subseteq k[x]$. □

Είμαστε σε θέση τώρα να αποδείξουμε το Θεώρημα 1.3.1.

**Απόδειξη του Θεωρήματος 1.3.1** Έστω $f(x) \in R[x]$, όπου ο $R$ είναι περιοχή μοναδικής παραγοντοποίησης. Υποθέτουμε ότι $f(x) \neq 0$ και επιπλέον δεν είναι αντιστρέψιμο. Αν $\deg f(x) = 0$, δεν έχουμε να αποδείξουμε τίποτα λόγω της υπόθεσης στο $R$. Έστω λοιπόν $\deg f(x) > 0$. Έστω $k$ το σώμα πηλίκων του $R$ (§ 0.7). Θεωρούμε $f(x) \in k[x]$. Λόγω του Παραδείγματος 1.1.6 έχουμε

$$f(x) = p_1(x)\cdots p_m(x), \quad p_i(x) \quad \text{ανάγωγο}.$$

Με απαλοιφή παρονομαστών παίρνουμε

$$df(x) = q_1(x)\cdots q_m(x), \quad d \in R, \quad q_i(x) \in R[x].$$

Κάθε $q_i(x)$ είναι ανάγωγο στο $k[x]$, γιατί $q_i(x) = u_i p_i(x)$ για κάποιο $u_i \in k$. Θεωρώντας περιεχόμενα έχουμε

$$f(x) = cg(x) \quad \text{και} \quad q_i(x) = c_i q_i'(x)$$

όπου $g(x), q_i'(x) \in R[x]$ είναι πρωταρχικά. Τότε

$$(dc)g(x) = (c_1\cdots c_m)q_i'(x)\cdots q_m'(x).$$

Το γινόμενο $q_i'(x)\cdots q_m'(x) \in R[x]$ είναι πρωταρχικό λόγω του Λήμματος του Gauss (Λήμμα 1.3.3). Τώρα από το Λήμμα 1.3.2 παίρνουμε

$$dcu = c_1\cdots c_m$$

για κάποιο αντιστρέψιμο $u \in R$. Επομένως

$$(dc)g(x) = (dcu)q_1'(x)\cdots q_m'(x)$$

και κατά συνέπεια

$$f(x) = cg(x) = (cu)q_1'(x)\cdots q_m'(x). \qquad (1)$$

Κάθε $q_i'(x)$ είναι ανάγωγο στο $R[x]$ λόγω του Λήμματος 1.3.4(ii). Επιπλέον το $cu \in R$ ή είναι αντιστρέψιμο ή γράφεται ως γινόμενο αναγώγων στοιχείων του $R$ λόγω της υπόθεσης στο $R$. Άρα η σχέση (1) δείχνει ότι το $f(x)$ αναλύεται σε γινόμενο αναγώγων παραγόντων στο $R[x]$. Θα δείξουμε στη συνέχεια τη μοναδικότητα της παραγοντοποίησης.

Έστω

$$f(x) = c_1 \cdots c_s p_1(x) \cdots p_m(x) = d_1 \cdots d_t q_1(x) \cdots q_n(x) \qquad (2)$$

δύο παραγοντοποιήσεις του $f(x)$ σε γινόμενα αναγώγων στοιχείων, όπου $c_i, d_j \in R$. Μπορούμε να υποθέσουμε ότι τα $p_i(x)$ και $q_j(x)$ είναι πρωταρχικά. Από το Λήμμα του Gauss, τα $p_1(x) \cdots p_m(x)$ και $q_1(x) \cdots q_n(x)$ είναι πρωταρχικά. Από το Λήμμα 1.3.2 τα στοιχεία $c_1 \cdots c_s$, $d_1 \cdots d_t$ είναι συντροφικά. Από τη μοναδικότητα της παραγοντοποίησης στο $R$ παίρνουμε $t = s$ και (μετά κάποια αναδιάταξη) κάθε $c_i$ είναι συντροφικό του $d_i$. Επειδή ο $R[x]$ είναι περιοχή, η σχέση (2) δίνει

$$p_1(x) \cdots p_m(x) = u q_1(x) \cdots q_n(x) \qquad (3)$$

για κάποιο αντιστρέψιμο $u \in R$. Θεωρούμε την (3) ως ισότητα στο $k[x]$. Από το Λήμμα 1.3.4(i) κάθε $p_i(x)$, $q_j(x)$ είναι ανάγωγο στο $k[x]$. Από τη μοναδικότητα της παραγοντοποίησης στο $k[x]$ (Παράδειγμα 1.1.6) παίρνουμε $m = n$ και (μετά από αναδιάταξη) κάθε $p_i(x)$ είναι συντροφικό του $q_i(x)$ στο $k[x]$. Άρα

$$p_i(x) = u_i q_i(x)$$

για κάποιο $u_i \in F$. Γράφοντας $u_i = \dfrac{a_i}{b_i}$ με $a_i, b_i \in R$ έχουμε

$$b_i p_i(x) = a_i q_i(x).$$

Από το Λήμμα 1.3.2 παίρνουμε $p_i(x) = v_i q_i(x)$ για κάποιο αντιστρέψιμο $v_i \in R$.

□

**1.3.5 Πόρισμα** *Οι δακτύλιοι* $\mathbb{Z}[x_1, \ldots, x_n]$ *και* $k[x_1, \ldots, x_n]$ *(k σώμα) είναι περιοχές μοναδικής παραγοντοποίησης.*

**Απόδειξη.** Επαγωγή στο *n* χρησιμοποιώντας το Θεώρημα 1.3.1 και το γεγονός ότι ο $\mathbb{Z}$ και ο *k* είναι περιοχές μοναδικής παραγοντοποίησης. □

## 1.4 Εφαρμογή: Τα Πρώτα Ιδεώδη του $\mathbb{Z}[x]$

Θα προσδιορίσουμε εδώ τα πρώτα ιδεώδη του $\mathbb{Z}[x]$.

Αν *R* είναι ένας δακτύλιος και $a \in R$ τότε ο επιμορφισμός

$$R \ni r \mapsto \bar{r} = r + (a) \in R/(a)$$

επάγει έναν επιμορφισμό

$$R[x] \ni f(x) = r_0 + \cdots + r_n x^n \mapsto \bar{f}(x) = \bar{r}_0 + \cdots + \bar{r}_n x^n \in R/(a)[x],$$

που έχει πυρήνα το ιδεώδες $(a)$ του $R[x]$. Η εικόνα του $f(x)$ ονομάζεται *αναγωγή* του $f(x)$ modulo *a*. (Την κατασκευή αυτή χρησιμοποιήσαμε στην απόδειξη του Λήμματος του Gauss).

**1.4.1 Πρόταση** *Κάθε πρώτο ιδεώδες P του* $\mathbb{Z}[x]$ *έχει μία από τις παρακάτω μορφές:*

*(i)* $P = (0)$

*(ii)* $P = (f)$ *για κάποιο ανάγωγο* $f \in \mathbb{Z}[x]$

*(iii)* $P = (p, f)$, *όπου* $p \in \mathbb{Z}$ *είναι πρώτος αριθμός και* $f \in \mathbb{Z}[x]$ *είναι τέτοιο ώστε η αναγωγή του f modulo p είναι ανάγωγο στο* $\mathbb{Z}_p[x]$.

*Τα ιδεώδη της περίπτωσης (iii) είναι τα μέγιστα ιδεώδη του* $\mathbb{Z}[x]$.

**Απόδειξη.** Ας αποδείξουμε πρώτα ότι τα παραπάνω ιδεώδη είναι πρώτα. Το (i) είναι άμεσο αφού ο $\mathbb{Z}[x]$ είναι περιοχή. Και το (ii) είναι άμεσο αφού ο $\mathbb{Z}[x]$ είναι δακτύλιος μονοσήμαντος παραγοντοποίησης (Θεώρημα 1.3.1). Για το (iii) παρατηρούμε ότι

$$\mathbb{Z}[x]/(p, f) \cong \mathbb{Z}_p[x]/(\bar{f}),$$

πράγμα που προκύπτει από το Θεώρημα 0.3.2 γιατί ο πυρήνας της σύνθεσης των επιμορφισμών $\mathbb{Z}[x] \to \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]/(\bar{f})$ είναι το ιδεώδες $(p, f)$. Τώρα ο

$\mathbb{Z}_p$ είναι σώμα (Πόρισμα 0.5.3) και συνεπώς ο $\mathbb{Z}_p[x]$ είναι περιοχή κυρίων ιδεωδών (Παράδειγμα 1.1.6). Από το Λήμμα 1.2.4, ο $\mathbb{Z}_p[x]/(\bar{f})$ είναι σώμα. Άρα (Πρόταση 0.6.4) το $(p, f)$ είναι μέγιστο ιδεώδες.

Έστω τώρα $P$ ένα πρώτο ιδεώδες του $\mathbb{Z}[x]$. Υποθέτουμε ότι το $P$ δεν είναι κύριο. Θα δείξουμε ότι είναι της μορφής (iii).

Έστω $g, h \in P$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι μ.κ.δ. $(g, h) = 1$. (Ως πρώτο, το $P$ περιέχει έναν ανάγωγο παράγοντα κάθε στοιχείο του. Αν όλοι αυτοί οι ανάγωγοι παράγοντες ταυτίζονταν, τότε το $P$ θα ήταν κύριο. Άρα υπάρχουν δύο διακεκριμένοι ανάγωγοι παράγοντες και προφανώς ο μ.κ.δ. αυτών είναι 1).

Και τώρα το λεπτό σημείο της απόδειξης:

*Ισχυρισμός: Για το ιδεώδες* $(g, h)$ *του* $\mathbb{Z}[x]$ *ισχύει* $(g, h) \cap \mathbb{Z} \neq (0)$.

Ας δεχτούμε προς στιγμή τον ισχυρισμό για να δούμε πως ολοκληρώνεται η απόδειξη της πρότασης. Έχουμε από τον ισχυρισμό $P \cap \mathbb{Z} \neq (0)$ και αφού το $P$ είναι πρώτο ιδεώδες υπάρχει πρώτος αριθμός $p \in P$. Θεωρούμε τον επιμορφισμό αναγωγή modulo $p$

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x].$$

Η εικόνα του $P$ είναι ιδεώδες του $\mathbb{Z}_p[x]$ γιατί ο $\varphi$ είναι επί. Ισχύει $\ker\varphi = (p) \subseteq P$. Με τη βοήθεια της σχέσης αυτής εύκολα ελέγχουμε ότι το ιδεώδες $\varphi(P)$ είναι πρώτο. Όμως ο $\mathbb{Z}_p[x]$ είναι περιοχή κυρίων ιδεωδών και συνεπώς $\varphi(P) = (\varphi(f))$ για κάποιο $f \in \mathbb{Z}[x]$. Εφόσον το ιδεώδες $(\varphi(f))$ είναι πρώτο, το $\varphi(f)$ είναι ανάγωγο στο $\mathbb{Z}_p[x]$. Θα δείξουμε τώρα ότι $P = (p, f)$. Έχουμε $\varphi(f) \in \varphi(P) \Rightarrow \varphi(f) = \varphi(a)$ για κάποιο $a \in P \Rightarrow f - a \in \ker\varphi \subseteq P \Rightarrow f \in P$ και άρα $(p, f) \subseteq P$. Για την άλλη σχέση, έστω $b \in P$. Τότε $\varphi(b) \in (\varphi(f)) \Rightarrow \varphi(b) = \varphi(c)\varphi(f)$ για κάποιο $c \in \mathbb{Z}[x] \Rightarrow b - cf \in \ker\varphi = (p) \Rightarrow b \in (p, f)$. Άρα $P \subseteq (p, f)$.

Δίνουμε τώρα την

*Απόδειξη του Ισχυρισμού*

Πρώτα θα δείξουμε ότι

$$\text{στο } \mathbb{Q}[x] \text{ ισχύει μ.κ.δ. } (g,h)=1. \qquad (1)$$

Έστω $g=dg_1$ και $h=dh_1$ με $d,g_1\in\mathbb{Q}[x]$ και $\deg d\geq 1$. Γράφουμε $d=ad_1$, $g_1=bg_2$, $h_1=ch_2$ με $a,b,c\in\mathbb{Q}$ και $d_1,g_2,h_2$ πρωταρχικά πολυώνυμα του $\mathbb{Z}[x]$. Από το Λήμμα του Gauss έχουμε ότι τα πολυώνυμα $d_1g_2$ και $d_1h_2$ είναι πρωταρχικά. Τώρα

$$g=dg_1=(ab)(d_1g_2)\in\mathbb{Z}[x].$$

Αλλά το $d_1g_2$ πρωταρχικά σημαίνει ότι $ab\in\mathbb{Z}$. Όμοια $ac\in\mathbb{Z}$. Συνεπώς $d_1\mid g$ και $d_1\mid h$ στο $\mathbb{Z}[x]$ που είναι άτοπο. Θα δείξουμε τώρα ότι $(g,h)\cap\mathbb{Z}\neq(0)$. Από την (1) και το γεγονός ότι ο $\mathbb{Q}[x]$ είναι περιοχή κυρίων ιδεωδών συμπεραίνουμε ότι υπάρχουν $r,s\in\mathbb{Q}[x]$ με την ιδιότητα

$$rg+sh=1 \qquad (2)$$

(Άσκηση 13). Απαλοίφοντας τους παρονομαστές των συντελεστών των $r$ και $s$ λαμβάνουμε από τη (2) μια σχέση της μορφής

$$(qr)g+(qs)h=q$$

όπου $q\in\mathbb{Z}-\{0\}$, $qr\in\mathbb{Z}[x]$ και $qs\in\mathbb{Z}[x]$. Άρα $q\in(g,h)\cap\mathbb{Z}$. □

Με παρόμοιο τρόπο αποδεικνύεται η παρακάτω πρόταση. (Αρκεί στη θέση του $\mathbb{Z}$ να θεωρήσουμε το $k[x]$ και στη θέση του $\mathbb{Q}$ να θεωρήσουμε το $k(x)$ έχοντας υπόψη ότι $k[x,y]=(k[x][y])$.

**1.4.2 Πρόταση** *Έστω k ένα σώμα. Κάθε πρώτο ιδεώδες P του $k[x,y]$ έχει μια από τις παρακάτω μορφές*

*(i)* $P=(0)$

*(ii)* $P=(f)$ *για κάποιο ανάγωγο* $f\in k[x,y]$

*(iii)* $P=(p,f)$, *όπου* $p\in k[x]$ *είναι ανάγωγο θετικού βαθμού και* $f\in k[x,y]$ *είναι τέτοιο ώστε η αναγωγή του f modulo p είναι ανάγωγο στο* $(k[x]/(p))[y]$. □

Στο σημείο αυτό θα πρέπει κάθε εκκολαπτόμενος Αλγεβριστής να διατυπώσει και να αποδείξει ένα θεώρημα που περιγράφει τα πρώτα ιδεώδη δακτυλίων της μορφής $R[x]$, όπου $R$ περιοχή κυρίων ιδεωδών.

## 1.5 Ευκλείδειες Περιοχές

Έχουμε διαπιστώσει ότι οι δακτύλιοι $\mathbb{Z}$ και $k[x]$ ($k$ σώμα) έχουν πολλές κοινές ιδιότητες. Μία απ' αυτές είναι η ταυτότητα διαίρεσης συνέπεια της οποίας είναι ότι οι $\mathbb{Z}$ και $k[x]$ είναι περιοχές κυρίων ιδεωδών (Παράδειγμα 1.1.6). Εδώ θα μελετήσουμε περιοχές που έχουν μια "ταυτότητα διαίρεσης". Αυτές ονομάζονται Ευκλείδειες περιοχές. Ακριβέστερα έχουμε:

**1.5.1 Ορισμός** *Μια Ευκλείδεια περιοχή είναι μία ακέραια περιοχή $R$ εφοδιασμένη με μία συνάρτηση $\varphi : R-\{0\} \to \mathbb{N}$, τέτοια ώστε*

*(i)* $a,b \in R$ *με* $a \mid b \Rightarrow \varphi(a) \le \varphi(b)$

*(ii)* $a \in R$ *και* $b \in R-\{0\}$. *Τότε υπάρχουν* $q,r \in R$ *με την ιδιότητα* $a = bq + r$ *και είτε* $r = 0$ *είτε* $\varphi(r) < \varphi(b)$.

Η συνάρτηση $\varphi$ ονομάζεται Ευκλείδεια συνάρτηση του $R$.

Για παράδειγμα έχουμε $R = \mathbb{Z}$ με $\varphi(m) = \mid m \mid$ (απόλυτη τιμή), και $R = k[x]$ ($k$ σώμα) με $\varphi(f(x)) = \deg f(x)$ (βαθμός πολυωνύμου). Σημειώνουμε ότι σε μια Ευκλείδεια περιοχή είναι δυνατόν να υπάρχουν πολλές Ευκλείδειες συναρτήσεις.

Το επόμενο αποτέλεσμα είναι σίγουρα αναμενόμενο.

**1.5.2 Πρόταση** *Κάθε Ευκλείδεια περιοχή είναι περιοχή κυρίων ιδεωδών.*

**Απόδειξη.** Έστω $I$ ιδεώδες της Ευκλείδειας περιοχής $R$ με $I \neq (0)$. Έστω $b \in I$ με την ιδιότητα $\varphi(b)$ είναι ελάχιστο. Θα δείξουμε ότι $I = (b)$. Αρκεί να δείξουμε $I \subseteq (b)$. Έστω $a \in I$. Έχουμε $a = bq + r$ όπου είτε $r = 0$ είτε $\varphi(r) < \varphi(b)$. Από τον ορισμό του $b$ συμπεραίνουμε ότι $r = 0$. Άρα $a = bq \in (a)$. □

Σημειώνουμε ότι δεν χρησιμοποιήσαμε την ιδιότητα (i) του ορισμού. Αυτή είναι συχνά χρήσιμη στον προσδιορισμό των αντιστρέψιμων στοιχείων μια Ευκλείδειας περιοχής, όπως δείχνει η παρακάτω πρόταση.

**1.5.3 Πρόταση** *Έστω R Ευκλείδεια περιοχή με Ευκλείδεια συνάρτηση φ. Τότε το* $u \in R$ *είναι αντιστρέψιμο αν και μόνο αν* $\varphi(u) = \varphi(1)$.

**Απόδειξη.** Αν $uv = 1$ τότε $\varphi(u) \le \varphi(1)$. Από την άλλη μεριά έχουμε $1 \mid u$ και άρα $\varphi(1) \le \varphi(u)$. Άρα $\varphi(u) = \varphi(1)$. Αντίστροφα, έστω $\varphi(u) = \varphi(1)$. Τότε υπάρχουν $q, r \in R$ με την ιδιότητα $1 = uq + r$ και είτε $r = 0$ είτε $\varphi(r) < \varphi(u)$. Αν $r \neq 0$, τότε $1 \mid r$ και $\varphi(1) \le \varphi(r)$ άτοπο. Άρα $r = 0$ και $1 = uq$. □

Το αντίστροφο της Πρότασης 1.5.2 δεν ισχύει, δηλαδή υπάρχουν περιοχές κυρίων ιδεωδών που δεν είναι Ευκλείδειες περιοχές. Ένα τέτοιο παράδειγμα είναι ο δακτύλιος $\left\{ \frac{a}{2} + \frac{b}{2}\sqrt{-19} \mid a, b \in \mathbb{Z} \quad \text{και} \quad a \equiv b \bmod 2 \right\}$. Η απόδειξη χρησιμοποιεί μέσα που ξεφεύγουν από τις σημειώσεις αυτές και παραλείπεται.

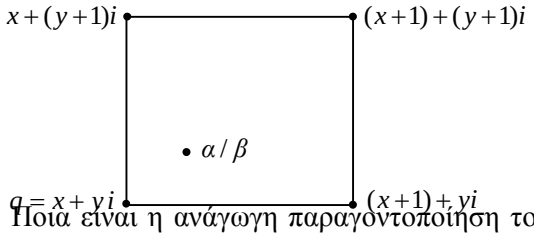
**1.5.4 Πρόταση** *Οι ακέραιοι του Gauss* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ *είναι Ευκλείδεια περιοχή. Τα αντιστρέψιμα στοιχεία του* $\mathbb{Z}[i]$ *είναι* $\{\pm 1, \pm i\}$.

**Απόδειξη.** Έστω $\varphi(a + b) = (a + bi)(a - bi) = a^2 + b^2$. Τότε $\varphi((a + bi)(c + di)) = \varphi(a + bi)\varphi(c + di)$. Κατά συνέπεια ισχύει η συνθήκη (i) του Ορισμού 1.5.1. Για τη συνθήκη (ii) τώρα, έστω $\alpha, \beta \in \mathbb{Z}[i]$ με $\beta \neq 0$. Θεωρούμε τον μιγαδικό αριθμό $\alpha / \beta$. Στο επίπεδο απεικονίζουμε τα στοιχεία του $\mathbb{Z}[i]$ στα σημεία με ακέραιες συντεταγμένες. Έτσι δημιουργούνται πολλά τετράγωνα με κορυφές τα παραπάνω σημεία και μήκος πλευράς 1. Επειδή το μήκος κάθε διαγωνίου είναι $\sqrt{2}$, συμπεραίνουμε ότι υπάρχει κορυφή που απέχει από το $\alpha / \beta$ απόσταση $\le \frac{\sqrt{2}}{2}$. Έστω $q$ μια τέτοια κορυφή. Τότε $|\alpha / \beta - q| \le \sqrt{2}/2 < 1$. Θέτοντας $r = \alpha - \beta q$ έχουμε

$$\alpha = \beta q + r \quad \text{και} \quad |r| = |\alpha - \beta q| = |\beta|\,|\alpha / \beta - q| < |\beta|.$$

Επομένως $\varphi(r) = |r|^2 < |\beta|^2 = \varphi(\beta)$.

Για τις μονάδες έχουμε (Πρόταση 1.5.3): $u$ μονάδα $\Leftrightarrow \varphi(u)=\varphi(1)=1$. Άρα $u=\pm 1$ και $\pm i$




**1.5.5 Παράδειγμα** Ποια είναι η ανάγωγη παραγοντοποίηση του $-1+7i \in \mathbb{Z}[i]$; (Ο $\mathbb{Z}[i]$ είναι περιοχή μοναδικής παραγοντοποίησης από την Πρόταση 1.5.2 και το Θεώρημα 1.2.1). Πρώτα μια γενική παρατήρηση: αν $\alpha \in \mathbb{Z}[i]$ είναι τέτοιο ώστε $\varphi(\alpha)=p$ πρώτος αριθμός στο $\mathbb{Z}$, τότε ο $\alpha$ είναι ανάγωγο. Πράγματι, αν $\alpha=\beta\gamma$, τότε $\varphi(\alpha)=\varphi(\beta)\varphi(\gamma)=p$ και άρα $\varphi(\beta)=1$ ή $\varphi(\gamma)=1$ δηλαδή $\beta$ αντιστρέψιμο ή $\gamma$ αντιστρέψιμο (Πρόταση 1.5.3). Τώρα στο συγκεκριμένο παράδειγμα. Έχουμε $\varphi(-1+7i)=50$. Αν ο $\alpha \in \mathbb{Z}[i]$ διαιρεί το $-1+7i$ θα πρέπει το $\varphi(\alpha)$ να διαιρεί το 50. Εξαιρώντας τις τετριμμένες περιπτώσεις, αναζητούμε τα $\alpha$ που ικανοποιούν $\varphi(\alpha)=2,5,10,25$. Κάποια απ' αυτά (όχι αναγκαστικά όλα) θα είναι διαιρέτες του $-1+7i$. Για $\varphi(\alpha)=2$ δοκιμάζουμε αν το $1+i$ είναι διαιρέτης του $-1+7i$. Εκτελώντας τη διαίρεση στο $\mathbb{C}$, βλέπουμε ότι το πηλίκο είναι στο $\mathbb{Z}[i]$, $-1+7i=(1+i)(3+4i)$. Το $1+i$ είναι ανάγωγο. Εκτελούμε την ίδια διαδικασία για το $3+4i$. Τελικά $-1+7i=(1+i)(2+i)^2$ είναι ανάγωγη παραγοντοποίηση.

**1.5.6 Παράδειγμα** Για κάθε $\alpha \in \mathbb{Z}[i]$, $\alpha \neq 0$, ο δακτύλιος $\mathbb{Z}[i]/(\alpha)$ είναι πεπερασμένος. Πράγματι κάθε στοιχείο του $\mathbb{Z}[i]/(\alpha)$ έχει τη μορφή $\beta+(\alpha)$ με $\beta \in \mathbb{Z}[i]$. Έχουμε $\beta=\alpha q+r$ με $q,r \in \mathbb{Z}[i]$ και είτε $r=0$ είτε $\varphi(r)<\varphi(\alpha)$. Τότε $\beta+(\alpha)=(\alpha)$ αν $r=0$, ή $\beta+(\alpha)=\varphi(r)+(\alpha)$. Το πλήθος όμως των $r \in \mathbb{Z}[i]$ που ικανοποιούν $\varphi(r)<\varphi(\alpha)$ για σταθερό $\alpha$ είναι προφανώς πεπερασμένο. □

## Ασκήσεις

**1*.** Ο δακτύλιος $R$ περιοχή κυρίων ιδεωδών. Τότε κάθε μη μηδενικό πρώτο ιδεώδες του $R$ είναι μέγιστο (Υπόδειξη: Λήμμα 1.2.4).

**2.** Χρησιμοποιήστε το Λήμμα 1.2.2 για να αποδείξετε ότι σε περιοχή κυρίων ιδεωδών κάθε γνήσιο ιδεώδες περιέχεται σε μέγιστο ιδεώδες. (Δες και το Πόρισμα 3.5.3).

**3.** Ποια είναι η ανάλυση του $x^3 - y^3 \in \mathbb{Q}[x, y]$ σε γινόμενο αναγώγων πολυωνύμων;

**4.** Η ακέραια περιοχή $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ δεν είναι περιοχή μοναδικής παραγοντοποίησης.

(Υπόδειξη $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$).

**5.** Έστω $k$ σώμα. Ο δακτύλιος $k[x]$ δεν είναι περιοχή κυρίων ιδεωδών.

**6.** Σωστό (απαιτείται απόδειξη) ή Λάθος (απαιτείται αντιπαράδειγμα)

(i) $R$ περιοχή κυρίων ιδεωδών $\Rightarrow R[x]$ περιοχή κυρίων ιδεωδών

(ii) $R$ περιοχή μοναδικής παραγοντοποίησης $\Rightarrow$ κάθε πρώτο ιδεώδες του $R$ είναι και μέγιστο

(iii) $R$ περιοχή μοναδικής παραγοντοποίησης $\Leftrightarrow R[x]$ περιοχή μοναδικής παραγοντοποίησης.

**7.** Έστω $R$ ακέραια περιοχή και $p \in R$ ένα μη μηδενικό μη αντιστρέψιμο στοιχείο. Το $p$ λέγεται πρώτο αν: $p \mid ab \Rightarrow p \mid a$ ή $p \mid b$.

(i) Αποδείξτε ότι κάθε πρώτο στοιχείο είναι ανάγωγο

(ii) Αν ο $R$ είναι περιοχή μοναδικής παραγοντοποίησης, τότε κάθε ανάγωγο στοιχείο είναι πρώτο.

**8.** Μια ακέραια περιοχή $R$ είναι περιοχή μοναδικής παραγοντοποίησης αν και μόνον αν

(i) Ισχύει η συνθήκη (i) του Ορισμού 1.1.3, και

(ii) Κάθε ανάγωγο στοιχείο είναι πρώτο (δες την προηγούμενη άσκηση). είναι και μέγιστο

**9.** Έστω $R$ περιοχή κυρίων ιδεωδών και $p \in R - \{0\}$. Τα ακόλουθα είναι ισοδύναμα

(i) $p$ είναι πρώτο στοιχείο (δες άσκηση 7)

(ii) $p$ είναι ανάγωγο στοιχείο

(iii) $R/(p)$ είναι σώμα

(iv) $R/(p)$ είναι ακεραία περιοχή.

**10.** Έστω $R$ περιοχή κυρίων ιδεωδών, $S$ ακέραια περιοχή και $\varphi: R \to S$ επιμορφισμός δακτυλίων. Τότε ο $\varphi$ είναι ισομορφισμός ή το $S$ είναι σώμα.

**11.** Γνωρίζουμε ότι $R$ σώμα $\Rightarrow R[x]$ περιοχή κυρίων ιδεωδών. Δείξτε το αντίστροφο: Έστω $R$ δακτύλιος (μεταθετικός με 1, όπως πάντα). Αν ο δακτύλιος $R[x]$ είναι περιοχή κυρίων ιδεωδών, τότε το $R$ είναι σώμα. (Υπόδειξη: θεωρήστε έναν επιμορφισμό $R[x] \to R$).

**12.** Ποια είναι τα πρώτα ιδεώδη του δακτυλίου $\mathbb{R}[x]$; Του $\mathbb{C}[x]$;

**13.** Έστω $R$ περιοχή κυρίων ιδεωδών και $a, b \in R$ όχι και τα δύο μηδέν. Τότε $(a,b) = (d)$, όπου $d = \text{μ.κ.δ.}(a,b)$.

**14.** Διατυπώστε και αποδείξετε μια πιο γενική μορφή του κριτηρίου του Eisenstein (Άσκηση 0.18) που ισχύει για τυχαία περιοχή μοναδικής παραγοντοποίησης στη θέση του $\mathbb{Z}$.

**15.** Έστω $R$ ακέραια περιοχή και $p \in R$

(i) $p$ είναι ανάγωγο αν και μόνο αν το ιδεώδες $(p)$ είναι μέγιστο στοιχείο του συνόλου των γνησίων κυρίων ιδεωδών του $R$ (Συγκρίνετε με το Λήμμα 1.2.4).

(ii) Δώστε ένα παράδειγμα $p \in R$ όπου το $p$ είναι ανάγωγο αλλά το ιδεώδες $(p)$ δεν είναι μέγιστο (Υπόδειξη: παράδειγμα 1.1.4).

**16.** Ο Δακτύλιος $\mathbb{R}[[t]]$ (§ 0.2) είναι περιοχή μοναδικής παραγοντοποίησης.

**17.** Βρείτε το $m \in \mathbb{N}$ έτσι ώστε $\mathbb{Z}[i]/(1+3i) \cong \mathbb{Z}_m$.

**18.** Στο $\mathbb{Z}[i]$ ισχύει $10 = 2 \cdot 5 = (1+3i)(1-3i)$ αλλά ο $\mathbb{Z}[i]$ είναι περιοχή μοναδικής παραγοντοποίησης. Εξηγήσετε.

**19.** Έστω $p \in \mathbb{Z}$ πρώτος αριθμός. Τα ακόλουθα είναι ισοδύναμα

(i) $p \in \mathbb{Z}[i]$ είναι πρώτο στοιχείο (άσκηση 7)

(ii) είναι σώμα

(iii) $x^2 + 1$ είναι ανάγωγο στο $\mathbb{Z}_p[x]$.

**20*.** Σε κάθε περιοχή κυρίων ιδεωδών κάθε γνήσιο ιδεώδες γράφεται ως γινόμενο πρώτων ιδεωδών.

**21.** (i) Η περιοχή $\mathbb{Z}[\sqrt{-2}]$ είναι Ευκλείδεια.

(ii) Οι λύσεις της Διοφαντικής εξίσωσης $y^2 + 2 = x^3$ είναι $x = 3$, $y = \pm 5$.

# Κεφάλαιο 2

# Επίπεδες Καμπύλες
# Μια πρώτη γεύση Αλγεβρικής Γεωμετρίας

Στο κεφάλαιο αυτό θα χρησιμοποιήσουμε το παράδειγμα των επίπεδων καμπύλων για να εισάγουμε μερικές βασικές έννοιες της Αλγεβρικής Γεωμετρίας, να διατυπώσουμε μερικά σημαντικά προβλήματά της και να περιγράψουμε τη γόνιμη αλληλεπίδραση Μεταθετικής Άλγεβρας και Αλγεβρικής Γεωμετρίας.

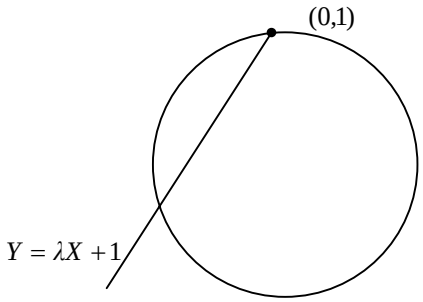
## 2.1 Ρητές Καμπύλες

Θεωρούμε ένα απλό πρόβλημα που όλοι μας έχουμε μελετήσει στο Λύκειο.

**2.1.1 Πρόβλημα** Να βρεθούν όλες οι ακέραιες λύσεις της εξίσωσης $x^2 + y^2 = z^2$.

Εξαιρώντας την τετριμμένη λύση $(0,0,0)$, θέτουμε $X = \frac{x}{z}$ και $Y = \frac{y}{z}$, οπότε ζητάμε τις ρητές λύσεις της

$$X^2 + Y^2 = 1 \qquad (1)$$



Η ευθεία $Y = \lambda X + 1$ τέμνει τον κύκλο (1) στα σημεία $(0,1)$ και $(X,Y) = \left( \frac{-2\lambda}{1+\lambda^2}, \frac{1-\lambda^2}{1+\lambda^2} \right)$. Παρατηρούμε ότι τα ρητά σημεία της (1), με την εξαίρεση του $(0,-1)$, βρίσκονται σε $1-1$ αντιστοιχία με τους ρητούς αριθμούς $\lambda \in \mathbb{Q}$. Έτσι βρίσκουμε όλες τις ρητές λύσεις της (1). Θέτοντας $\lambda = m/n$ όπου $m,n \in \mathbb{Z}$ παίρνουμε όλες τις λύσεις της αρχικής εξίσωσης: είναι ακέραια πολλαπλάσια λύσεων της μορφής $(-2mn, n^2 - m^2, m^2 + n^2)$ ("τριάδες του Πυθαγόρα").

Με παρόμοιο τρόπο μπορεί να αποδειχθεί ότι κάθε ακέραια λύση της $2x^2 + y^2 = 9z^2$ είναι πολλαπλάσιο μιας λύσης της μορφής $x = -6mn$, $y = -3m^2 + 6n^2$, $z = m^2 + 2n^2$ (άσκηση).

Τα παραδείγματα αυτά δείχνουν ότι η παραμετρικοποίηση καμπυλών συχνά βοηθά στην επίλυση Διοφαντικών εξισώσεων. Έτσι οδηγούμαστε σ' ένα από τα σημαντικά ερωτήματα της Αλγεβρικής Γεωμετρίας.

### 2.1.2 Ερώτημα *Ποιες καμπύλες επιδέχονται ρητές παραμετρικοποιήσεις;*

Πριν ασχοληθούμε με το προηγούμενο ερώτημα πιο αναλυτικά δίνουμε μερικούς ορισμούς. Έστω $k$ ένα σώμα και $f(x,y) \in k[x,y]$ ένα πολυώνυμο με συντελεστές από το $k$. Το σύνολο των σημείων $(\alpha,\beta) \in k^2$ που ικανοποιούν τη σχέση $f(\alpha,\beta) = 0$ ονομάζεται (επίπεδη) *καμπύλη* και συμβολίζεται με $C_f$. Θα λέμε ότι η $C_f$ είναι *ανάγωγη* αν το $f(x,y)$ είναι ανάγωγο στο $k[x,y]$. Υπενθυμίζουμε ότι ο $k[x,y]$ είναι περιοχή μοναδικής παραγοντοποίησης (Πόρισμα 1.3.5). Αν $f = g,h$ με $f,g,h \in k[x,y]$, τότε $C_f = C_g \cup C_h$. Συνεπώς κάθε καμπύλη είναι ένωση πεπερασμένου πλήθους αναγώγων καμπυλών, μια για κάθε ανάγωγο παράγοντα του $f$. Έτσι θα επικεντρώσουμε την προσοχή μας στην περίπτωση που το $f(x,y)$ είναι ανάγωγο στο $k[x,y]$. Ο *βαθμός* μιας ανάγωγης καμπύλης είναι ο βαθμός του αντίστοιχου πολυωνύμου. Κάθε ανάγωγη καμπύλη βαθμού 2 ή 3 λέγεται *κωνική* ή *κυβική* αντίστοιχα. Μια καμπύλη λέγεται *ρητή* αν υπάρχουν ρητές συναρτήσεις $\alpha(t), \beta(t) \in k(t)$, από τις οποίες μια τουλάχιστον δεν

είναι σταθερή, έτσι ώστε $f(\alpha(t),\beta(t))\equiv 0$ (ταυτοτικά μηδέν ως ρητή συνάρτηση στο $t$). Θα λέμε τότε ότι $x\mapsto\alpha(t)$ και $y\mapsto\beta(t)$ είναι μια *ρητή παραμετρικοποίηση* της $C_f$. Έτσι το ερώτημά μας είναι: Ποιες καμπύλες είναι ρητές;

Προφανώς κάθε καμπύλη βαθμού 1 είναι ρητή. Αποδεικνύεται ότι κάθε κωνική είναι ρητή (βλ. Άσκηση 3). Η κυβική $C_f$, $f=y^2-x^3$, είναι επίσης ρητή $(\alpha(t)=t^2,\beta(t)=t^3)$. Αντίθετα οι καμπύλες του Fermat $x^n+y^n=1$ δεν είναι γενικά ρητές. Ακριβέστερα έχουμε:

**2.1.3 Πρόταση** *Έστω* $k=\mathbb{C}$. *Η καμπύλη του Fermat που ορίζεται από* $x^n+y^n=1$ *είναι ρητή αν και μόνο αν* $n\le 2$.

**Απόδειξη.** Έστω ότι η καμπύλη $x^n+y^n=1$ είναι ρητή. Τότε υπάρχουν πολυώνυμα $f,g,h\in k[t]$, τέτοια ώστε μ.κ.δ.$(f,g,h)=1$ και $f^n+g^n=h^n$. Αν $a,b,c$ είναι οι αντίστοιχοι βαθμοί των $f$, $g$ και $h$, μπορούμε να υποθέσουμε ότι $a\ge b$ και $a\ge c$. Παραγωγίζοντας παίρνουμε $ff'^{n-1}+g'g^{n-1}=h'h^{n-1}$ (εδώ χρησιμοποιούμε ότι η χαρακτηριστική του $k$ είναι μηδέν). Οι δύο σχέσεις δίνουν $f^{n-1}(fg'-f'g)=h^{n-1}(hg'-h'g)$. Εφόσον μ.κ.δ.$(f,h)=1$, παίρνουμε $f^{n-1}$ διαιρεί το $hg'-h'g$. Άρα $(n-1)a\le b+c-1$. Αλλά $b\le a$ και $c\le a$. Έτσι παίρνουμε $(n-1)a\le 2a-1$. Συνεπώς $n\le 2$.

Αντίστροφα, έστω $n=2$. Μια ρητή παραμετρικοποίηση είναι $x\mapsto\dfrac{2t}{1+t^2}$, $y\mapsto\dfrac{1-t^2}{1+t^2}$. □

Ένα άμεσο πόρισμα είναι το εξής:

**2.1.4 Πόρισμα** *(Θεώρημα του Fermat για πολυώνυμα). Έστω* $n\ge 3$. *Τότε δεν υπάρχουν πολυώνυμα* $f,g,h\in\mathbb{C}[x]$ *θετικού βαθμού με μ.κ.δ.*$(f,g)=1$ *έτσι ώστε* $f^n+g^n=h^n$. □

Η επόμενη πρόταση θα χρησιμοποιηθεί πολλές φορές σ' αυτό το κεφάλαιο.

**2.1.5 Πρόταση** *Έστω* $f, g \in k[x, y]$ *με f ανάγωγο. Αν το g δεν διαιρείται με το f, τότε το σύστημα*

$$f(x, y) = g(x, y) = 0$$

*έχει πεπερασμένο το πλήθος λύσεις.*

**Απόδειξη.** Θεωρούμε τα πολυώνυμα $f, g$ ως στοιχεία του $k(y)[x]$, δηλαδή πολυώνυμα στη μεταβλητή $x$ με συντελεστές ρητές συναρτήσεις του $y$ και υποθέτουμε ότι ο βαθμός του $f$ ως προς $x$ είναι $> 0$. Τότε το $f$ παραμένει ανάγωγο και εξακολουθεί να μη διαιρεί το $g$ στο $k(y)[x]$ (γιατί;). Άρα μ.κ.δ. $(f, g) = 1$ στο $k(y)[x]$. Αλλά ο $k(y)[x]$ είναι περιοχή κυρίων ιδεωδών αφού του $k(y)$ είναι σώμα (Παράδειγμα 1.1.6). Άρα (Άσκηση 1.13) υπάρχουν $\bar{f}, \bar{g} \in k(y)[x]$ με την ιδιότητα

$$f\,\bar{f} + g\,\bar{g} = 1.$$

Απαλοίφοντας τους παρονομαστές των $\bar{f}, \bar{g}$ παίρνουμε μια σχέση της μορφής

$$f\,\tilde{f} + g\,\tilde{g} = h$$

όπου $h \in k[y]$ και $\tilde{f}, \tilde{g} \in k[x, y]$. Αν $f(\alpha, \beta) = g(\alpha, \beta) = 0$ για κάποιο $(\alpha, \beta) \in k^2$, τότε $h(\beta) = 0$. Αφού το $h$ είναι μη μηδενικό πολυώνυμο μιας μεταβλητής, υπάρχουν πεπερασμένες το πλήθος δυνατότητες για τις τιμές του $\beta$. Εναλλάσσοντας τους ρόλους των $x$ και $y$ φτάνουμε στο ίδιο συμπέρασμα για τις τιμές του $\alpha$. □

**2.1.6 Πόρισμα** *Αν το σώμα k είναι αλγεβρικά κλειστό (§ 0.8),* $f, g \in k[x, y]$ *με f ανάγωγο και* $C_f \subseteq C_g$*, τότε το f διαιρεί το g στο* $k[x, y]$.

**Απόδειξη.** Η καμπύλη $C_f$ έχει άπειρα σημεία αφού το $k$ είναι αλγεβρικά κλειστό (γιατί;). Άρα το σύστημα $f(x, y) = g(x, y) = 0$ έχει άπειρες λύσεις. Από την Πρόταση 2.1.5 παίρνουμε ότι το $g$ διαιρείται από το $f$.

□

**Σημείωση.** (i) Οι αναγνώστες που είναι έμπειροι στη Μεταθετική Άλγεβρα θα αναγνωρίσουν ότι το Πόρισμα 2.1.6 είναι μια ειδική περίπτωση του Nullstellensatz (Δες Κεφάλαιο 8).

(ii) Το Πόρισμα 2.1.6 δεν ισχύει γενικά αν το *k* δεν είναι αλγεβρικά κλειστό: για παράδειγμα, αν $f = x^2 + y^2$, $g = x^4 + y^4 \in \mathbb{R}[x, y]$ τότε $C_f = C_g = \{(0,0)\}$. Όμως υπάρχουν πολύ ενδιαφέροντα προβλήματα που αφορούν καμπύλες που ορίζονται πάνω από μη αλγεβρικά κλειστά σώματα *k* όπως: ρητές λύσεις πολυωνυμικών εξισώσεων $(k = \mathbb{C})$ ή λύσεις πολυωνυμικών ισοδυναμιών $(k = \mathbb{Z}_p)$.

(iii) Το Πόρισμα 2.1.6 μας πληροφορεί ότι ο βαθμός ανάγωγης καμπύλης είναι μονοσήμαντα ορισμένος όταν το *k* είναι αλγεβρικά κλειστό.

## 2.2 Ρητές Καμπύλες και Υπερβατικές Επεκτάσεις

Θα δώσουμε εδώ μια απάντηση στο Ερώτημα 2.1.2. Η μεθοδολογία είναι τυπική για την Αλγεβρική Γεωμετρία: Για κάθε καμπύλη *C* θα ορίσουμε ένα αλγεβρικό αντικείμενο, το σώμα των ρητών συναρτήσεων πάνω στη *C*. Αλγεβρικές ιδιότητες του σώματος αυτού αντανακλούν γεωμετρικές ιδιότητες της καμπύλης.

Πρώτα όμως θα υπενθυμίσουμε μερικούς ορισμούς. Έστω $E/F$ επέκταση σωμάτων, δηλαδή τα *E* και *F* είναι σώματα με $F \subseteq E$. Ένα στοιχείο $\alpha \in E$ λέγεται *αλγεβρικό* πάνω από το *F* αν είναι ρίζα μη μηδενικού πολυωνύμου με συντελεστές από το *F*. Το $\alpha \in E$ λέγεται *υπερβατικό* πάνω από το *F* αν δεν είναι αλγεβρικό πάνω από το *F*. Για παράδειγμα η "μεταβλητή" *t* του σώματος $\mathbb{R}(t)$ είναι υπερβατικό πάνω από το $\mathbb{R}$. Επίσης το $\pi \in \mathbb{R}$ είναι $e \in \mathbb{R}$ είναι υπερβατικά πάνω από το $\mathbb{Q}$ (Lindermann 1882 και Hermite 1873 αντίστοιχα). Μία επέκταση $E/F$ λέγεται *υπερβατική* αν το *E* περιέχει ένα τουλάχιστον υπερβατικό στοιχείο πάνω από το *F*.

Έστω $C_f$ μια ανάγωγη καμπύλη. Το κύριο ιδεώδες $(f) \subseteq k[x, y]$ είναι πρώτο γιατί το $f$ είναι ανάγωγο και το $k[x, y]$ είναι περιοχή μοναδικής παραγοντοποίησης (Πόρισμα 1.3.5). Έτσι ο δακτύλιος $k[x, y]/(f)$ είναι περιοχή και μπορούμε να θεωρήσουμε το σώμα πηλίκων του.

**2.2.1 Ορισμός** *Με τους προηγούμενους συμβολισμούς ορίζουμε*

*(i)* $k[C_f] = k[x,y]/(f)$, *που ονομάζεται δακτύλιος συντεταγμένων της* $C_f$.

*(ii)* $k(C_f) =$ *σώμα πηλίκων του* $k[C_f]$, *που ονομάζεται σώμα των ρητών συναρτήσεων στη* $C_f$.

**2.2.2 Παράδειγμα** (i) Έστω η παραβολή $C_f$, $f = y - x^2$. Τότε $k[C_f] = k[x,y]/(y-x^2) \cong k[x]$ (γιατί;) και $k(C_f) \cong k(x)$.

(ii) Έστω η κυβική $C_g$, $g = y^2 - x^3$, όπου $k$ είναι αλγεβρικά κλειστό. Θα δείξουμε ότι $k[C_g] \cong k[t^2, t^3]$. Η παραμετρικοποίηση $x \mapsto t^2$, $y \mapsto t^3$ ορίζει έναν επιμορφισμό δακτυλίων

$$\varphi : k[x,y] \to k[t^2, t^3].$$

Προφανώς $\ker\varphi \supseteq (y^2 - x^3)$. Ισχυριζόμαστε ότι $\ker\varphi = (y^2 - x^3)$. Έστω $h \in \ker\varphi$. Τότε το σύστημα

$$y^2 - x^3 = h = 0$$

έχει άπειρες λύσεις, τα σημεία της $C_g$ (το $k$ είναι αλγεβρικά κλειστό). Από την Πρόταση 2.1.5 παίρνουμε ότι το $y^2 - x^3$ διαιρεί το $h$, δηλαδή $h \in (y^2 - x^3)$. Τώρα από τη σχέση $\ker\varphi = (y^2 - x^3)$ και τον επιμορφισμό $\varphi$ παίρνουμε (Θεώρημα 0.3.2) $k[x,y]/(y^2 - x^3) \cong k[t^2, t^3]$. Απ' αυτό έπεται εύκολα ότι $k(C_g) \cong k(t)$.

**Σημείωση.** (i) Το κίνητρο που οδήγησε στον ορισμό του δακτυλίου συντεταγμένων μπορεί να εξηγηθεί ως εξής: Ένας τρόπος μελέτης μιας ανάγωγης καμπύλης $C_f \subseteq k^2$, όπου $k$ αλγεβρικά κλειστό, είναι η μελέτη των περιορισμών στη $C_f$ των πολυωνυμικών συναρτήσεων $k^2 \to k$. Έστω $g, h : k^2 \to k$ δύο πολυωνυμικές συναρτήσεις. Τότε οι περιορισμοί τους στη $C_f$ είναι ίσες αν και μόνο αν $g(c) = h(c)$ για κάθε $c \in C_f$, δηλαδή αν και μόνο αν η $g - h$ είναι μηδέν πάνω στη $C_f$. Αλλά τότε (Πρόταση 2.1.5) ισχύει: $g - h$ ανήκει στο ιδεώδες $(f)$.

Άρα στο δακτύλιο $k[x,y]/(f)$ ισχύει $g+(f)=h+(f)$. Μπορούμε λοιπόν να θεωρήσουμε κατά φυσικό τρόπο τα στοιχεία του $k[x,y]/(f)$ ως τους περιορισμούς στη $C_f \subseteq k^2$ των πολυωνυμικών συναρτήσεων $k^2 \to k$.

(ii) Θα χρησιμοποιήσουμε τον ίδιο συμβολισμό για $f(x,y) \in k[x,y]$ και την εικόνα του στο $k[C_g]$.

Δίνουμε τώρα μια απάντηση στο Ερώτημα 2.1.2. Δύο σώματα $E$ και $F$ που περιέχουν το σώμα $k$ λέγονται *k-ισόμορφα* αν υπάρχει ισομορφισμός σωμάτων $\varphi: E \to F$ με την ιδιότητα $\varphi(r)=r \ \ \forall\, r \in k$.

**2.2.3 Θεώρημα** *Έστω $k$ ένα αλγεβρικά κλειστό σώμα και $C_f$ μια ανάγωγη καμπύλη. Τότε η $C_f$ είναι ρητή αν και μόνο αν το σώμα $k(C_f)$ είναι k-ισόμορφο με το σώμα $k(t)$.*

Για την απόδειξη θα εφαρμόσουμε το Θεώρημα του Lüroth:

**2.2.4 Θεώρημα** *(Lüroth). Έστω σώματα*

$$F \subsetneq E \subseteq F(t),$$

*όπου το $t$ είναι υπερβατικό πάνω από το $F$. Τότε $E = F(u(t))$ για κάποιο $u(t) \in F(t)$.*

Η απόδειξη του Θεωρήματος του Lüroth δεν χρησιμοποιεί τίποτα πέρα από τις στοιχειώδεις ιδιότητες επεκτάσεων σωμάτων. Όμως θα την παραλείψουμε για να μην επεκταθούμε σε άλλα θέματα.

**Απόδειξη του Θεωρήματος 2.2.3** Έστω ότι η $C_f$ είναι ρητή, δηλαδή υπάρχουν $\alpha(t), \beta(t) \in k(t)$, όχι και οι δύο σταθερές, έτσι ώστε $f(\alpha(t), \beta(t)) \equiv 0$. Ορίζουμε έναν ομομορφισμό *k*-σωμάτων,

$$\varphi: k(C_f) \ni \frac{p(x,y)}{q(x,y)} \mapsto \frac{p(a(t),\beta(t))}{q(\alpha(t),\beta(t))} \in k(t).$$

Παρατηρούμε ότι

(i) ο $\varphi$ είναι καλά ορισμένος: Πρώτα, αν $\frac{p(x,y)}{q(x,y)} = \frac{\tilde{p}(x,y)}{\tilde{q}(x,y)}$, τότε $p(x,y)\tilde{q}(x,y) = q(x,y)\tilde{p}(x,y) \in (f)$ οπότε $p(\alpha(t),\beta(t))\tilde{q}(\alpha(t),\beta(t)) - q(\alpha(t),\beta(t))\tilde{p}(\alpha(t),\beta(t)) \equiv 0$. Δεύτερο, αν $q(\alpha(t),\beta(t)) \equiv 0$, τότε το σύστημα $q(x,y) = f(x,y) = 0$ θα είχε άπειρες λύσεις (γιατί ο $k$ είναι αλγεβρικά κλειστό). Από την Πρόταση 2.1.5 έπεται ότι το $q(x,y)$ είναι πολλαπλάσιο του $f$. Ως στοιχείο του $k[C_f]$, θα είχαμε τότε $q(x,y) = 0$.

(ii) ο $\varphi$ είναι μονομορφισμός: αν $p(x,y) \mid q(x,y) \in \ker\varphi$, τότε $p(\alpha(t),\beta(t)) \equiv 0$ και όπως πριν συμπεραίνουμε ότι $p(x,y) = 0$ ως στοιχείο του $k[C_f]$.

Έχουμε λοιπόν έναν $k$-ισομορφισμό $k(C_f) \cong \mathrm{Im}\varphi$. Επιπλέον ισχύει $k \subsetneq \mathrm{Im}\varphi$, γιατί τουλάχιστον μια από τις $\alpha(t)$, $\beta(t)$ δεν είναι σταθερή. Από το Θεώρημα του Lüroth υπάρχει $u(t) \in k(t)$, έτσι ώστε $\mathrm{Im}\varphi = k(u(t))$. Τέλος παρατηρούμε ότι η αντιστοιχία $u(t) \mapsto t$ δίνει ένα $k$-ισομορφισμό σωμάτων $k(u(t)) \to k(t)$ γιατί η $u(t)$ δεν είναι σταθερή.

Αντίστροφα, έστω ότι υπάρχει $k$-ισομορφισμός $\varphi : k(C_f) \to k(t)$. Θέτοντας $\varphi(x) = \alpha(t)$ και $\varphi(y) = \beta(t)$ και εφαρμόζοντας στη σχέση $f(x,y) = 0$ (που είναι σχέση στο $k[C_f]$) τη $\varphi$ παίρνουμε $f(\alpha(t),\beta(t)) \equiv 0$ και $\alpha(t)$ ή $\beta(t)$ δεν είναι σταθερή. Άρα η $C_f$ είναι ρητή. □

Είδαμε στο πρόβλημα 2.1.1 ότι η συγκεκριμένη παραμετρικοποίηση έδωσε όλες τις ρητές λύσεις της $X^2 + Y^2 = 1$ εκτός από μία, τη $(0,-1)$. Έτσι γεννιέται το ερώτημα: κατά πόσο μια παραμετρικοποίηση "καταμετρά" όλα τα σημεία μιας ρητής καμπύλης. Η απάντηση δίνεται από την παρακάτω πρόταση.

Έστω $C_f$ ρητή καμπύλη και $\varphi : k(C_f) \cong k(t)$ ο ισομορφισμός σωμάτων που παρέχει το Θεώρημα 2.2.3. Θέτουμε $\varphi(x) = \alpha(t)$ και $\varphi(y) = \beta(t)$.

**2.2.5 Πρόταση** *(i) Εκτός ενδεχομένως από ένα πεπερασμένο πλήθος σημείων, κάθε* $(x_0, y_0) \in C_f$ *έχει μια παράσταση της μορφής* $(x_0, y_0) = (\alpha(t_0), \beta(t_0))$, *για κάποιο* $t_0 \in k$.

*(ii) Εκτός ενδεχομένως από ένα πεπερασμένο πλήθος σημείων, η παραπάνω παράσταση είναι μοναδική.*

**Απόδειξη.** Έχουμε ισομορφισμούς

$$k(C_f) \xrightarrow{\varphi} k(t) \xrightarrow{\varphi^{-1}} k(C_f).$$

Αν $\varphi^{-1}(t) = h(x, y)$, τότε έχουμε

$$x = \alpha(h(x, y)) \quad \text{και} \quad y = \beta(h(x, y)).$$

(i) Τώρα ο παρονομαστής του $h(x, y)$ μηδενίζεται το πολύ σε πεπερασμένο πλήθος σημεία της καμπύλης $C_f$ (Πρόταση 2.1.5 και πάλι).

(ii) Έχουμε $t = h(\alpha(t), \beta(t))$. Συνεπώς, αν υπάρχει $t_0$ έτσι ώστε $(x_0, y_0) = (\alpha(t_0), \beta(t_0))$, τότε αυτό είναι μοναδικό. □

Σημειώνουμε ότι η προηγούμενη πρόταση δεν ισχύει γενικά για όλες τις παραμετρικοποιήσεις. Για παράδειγμα, μια παραμετρικοποίηση της $y = x^2$ είναι $\alpha(t) = t^2$, $\beta(t) = t^4$. Όμως $t$ και $-t$ ορίζουν το ίδιο σημείο πάνω στην καμπύλη.

## 2.3 Ισομορφισμός Καμπυλών

Έστω $C_f$, $C_g$ δύο καμπύλες. Μια απεικόνιση

$$\varphi : C_f \to C_g$$

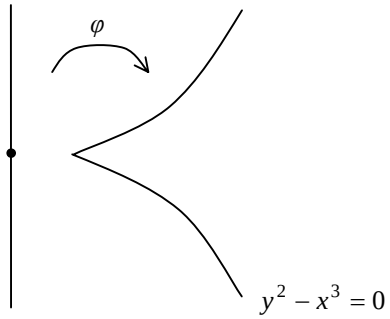
ονομάζεται *πολυωνυμική* αν υπάρχουν πολυώνυμα $u(x, y), v(x, y) \in k[x, y]$ με την ιδιότητα

$$\varphi(\alpha, \beta) = (u(\alpha, \beta), v(\alpha, \beta)) \quad \text{για κάθε} \quad (\alpha, \beta) \in C_f.$$

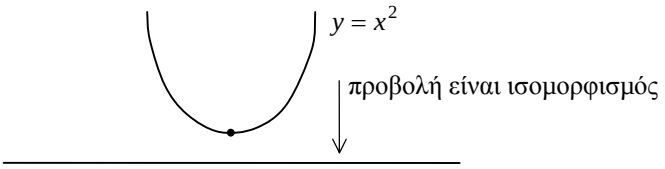
Μια πολυωνυμική απεικόνιση $\varphi : C_f \to C_g$ ονομάζεται *ισομορφισμός* αν υπάρχει πολυωνυμική απεικόνιση $\psi : C_g \to C_f$ έτσι ώστε $\psi \circ \varphi = 1_{C_f}$ και $\varphi \circ \psi = 1_{C_g}$. Θα λέμε τότε ότι οι καμπύλες $C_f$ και $C_g$ είναι *ισόμορφες*.

**2.3.1 Παράδειγμα** (i) Έστω $C_f$ η κυβική που ορίζεται από $f = y^2 - x^3$. Η παραμετρικοποίηση $\alpha(t) = t^2$ και $\beta(t) = t^3$ ορίζει μια πολυωνυμική απεικόνιση

$$\varphi : k \times \{0\} \ni (t,0) \mapsto (t^2, t^3) \in C_f$$




(ii) Έστω $C_g$ η παραβολή που ορίζεται από $g = y - x^2$. Η απεικόνιση $\varphi : k \times \{0\} \ni (t,0) \mapsto (t, t^2) \in C_g$ είναι πολυωνυμική. Μάλιστα είναι ισομορφισμός, γιατί αν $\psi : C_g \ni (x,y) \mapsto (x,0) \in k \times \{0\}$ είναι η προβολή στον άξονα των $x$, έχουμε $\psi \circ \varphi = 1_{k\times\{0\}}$ και $\varphi \circ \psi = 1_{C_g}$. Άρα η παραβολή $y - x^2 = 0$ είναι ισόμορφη με ευθεία.




**2.3.2 Θεώρημα** *Έστω $C_f$ και $C_g$ δύο ανάγωγες καμπύλες πάνω από ένα αλγεβρικά κλειστό σώμα k. Τότε αυτές είναι ισόμορφες αν και μόνον αν οι k-άλγεβρες $k[C_f]$ και $k[C_g]$ είναι ισόμορφες.*

Πριν δώσουμε την απόδειξη του προηγούμενου θεωρήματος επισημαίνουμε μια χρήσιμη παρατήρηση: Έστω $C_f$ μια ανάγωγη καμπύλη. Αν $h \in k[x,y]$, συμβολίζουμε με $\bar{h}$ τη συνάρτηση

$$\bar{h} : C_f \ni (\alpha, \beta) \mapsto h(\alpha, \beta) \in k .$$

Το σύνολο των $\bar{h}$, όταν $h \in k[x,y]$, συμβολίζουμε (προσωρινά) με $\bar{k}[C_f]$. Τα στοιχεία του ονομάζονται *πολυωνυμικές συναρτήσεις*. Είναι μια $k$-άλγεβρα με τις προφανείς πράξεις. Ο πυρήνας του επιμορφισμού $k$-αλγεβρών

$$k[x,y] \ni h(x,y) \mapsto \bar{h}(x,y) \in \bar{k}[x,y]$$

περιέχει προφανώς το κύριο ιδεώδες $(f)$. Επειδή το $f(x,y)$ είναι ανάγωγο και το $k$ αλγεβρικά κλειστό, η Πρόταση 2.1.5 μας δίνει ότι ο πυρήνας είναι το $(f)$. Εφαρμόζοντας το $1^{ο}$ Θεώρημα Ισομορφισμών Δακτυλίων (Θεώρημα 0.3.2), παίρνουμε

$$\bar{k}[C_f] \cong k[x,y]/(f) .$$

Αλλά ο δακτύλιος $k[x,y]/(f)$ είναι ο δακτύλιος συντεταγμένων του $C_f$. Άρα $\bar{k}[C_f] \cong k[C_f]$.

*Συμπέρασμα.* Θα ταυτίζουμε, χωρίς να γίνεται ιδιαίτερη μνεία, τα στοιχεία του δακτυλίου $k[C_f]$ με τις πολυωνυμικές συναρτήσεις $C_f \to k$.

**Απόδειξη του Θεωρήματος 2.2.2** Έστω ότι οι $C_f$ και $C_g$ είναι ισόμορφες. Για κάθε πολυωνυμική απεικόνιση $\varphi : C_f \to C_g$ ορίζεται ένας ομομορφισμός $k$-αλγεβρών,

$$\varphi^* : k[C_g] \to k[C_f], \quad \varphi^*(h) = h \circ \varphi .$$

Τώρα αν $\varphi : C_f \to C_g$ και $\psi : C_g \to C_f$ έχουν την ιδιότητα $\varphi \circ \psi = 1$ και $\psi \circ \varphi = 1$, τότε εύκολα αποδεικνύεται ότι $\psi^* \circ \varphi^* = 1$ και $\varphi^* \circ \psi^* = 1$.

Αντίστροφα, έστω $k[C_f] \cong k[C_g]$ ως $k$-άλγεβρες. Θα δείξουμε ότι κάθε ομομορφισμός $k$-αλγεβρών $k[C_g] \to k[C_f]$ είναι της μορφής $\varphi^*$ για μοναδική πολυωνυμική απεικόνιση $\varphi : C_f \to C_g$. Έστω λοιπόν $\Phi : k[C_g] \to k[C_f]$ ομομορφισμός $k$-αλγεβρών, και έστω $\bar{x}, \bar{y} : C_g \to k$ οι περιορισμοί στο $C_g$ της

πρώτης και δεύτερης προβολής αντίστοιχα. Έχουμε $\bar{x}, \bar{y} \in k[C_g]$ και άρα $\Phi(\bar{x}), \Phi(\bar{y}) \in k[C_f]$. Ορίζουμε την απεικόνιση

$$\varphi : C_f \ni P \mapsto \big(\Phi(\bar{x})(P), \Phi(\bar{y})(P)\big) \in k^2 .$$

Η $\varphi$ είναι προφανώς πολυωνυμική. Ισχυριζόμαστε ότι $\mathrm{Im}\,\varphi \subseteq C_g$. Πράγματι, αρκεί να δείξουμε ότι $g(\Phi(\bar{x})(P), \Phi(\bar{y})(P)) = 0$ για κάθε $P \in C_f$. Ισχύει $g(\bar{x}, \bar{y}) = 0$ στο $k[C_g]$ και άρα $\Phi(g(\bar{x}, \bar{y})) = 0$. Αλλά επιπλέον ισχύει

$$\Phi(g(\bar{x}, \bar{y})) = g(\Phi(\bar{x}), \Phi(\bar{y}))$$

αφού ο $\Phi$ είναι ομομορφισμός $k$-αλγεβρών. Άρα έχουμε $g(\Phi(\bar{x}), \Phi(\bar{y})) = 0 \in k[C_f]$. Συνεπώς $\mathrm{Im}\,\varphi \subseteq C_g$. Από τους ορισμούς εύκολα προκύπτει ότι για την απεικόνιση $\varphi : C_f \to C_g$ ισχύει $\varphi^* = \Phi$. Η μοναδικότητα της $\varphi$ προκύπτει επίσης άμεσα από τους ορισμούς.

Εφόσον τώρα $k[C_f] \cong k[C_g]$ υπάρχουν $\Phi : k[C_f] \to k[C_g]$ και $\Psi : k[C_g] \to k[C_f]$ με $\Phi \circ \Psi = 1$ και $\Psi \circ \Phi = 1$. Τότε υπάρχουν πολυωνυμικές απεικονίσεις $\varphi : C_g \to C_f$ και $\psi : C_f \to C_g$ με $\varphi^* = \Phi$ και $\psi^* = \Psi$. Συνεπώς

$$\varphi^* \circ \psi^* = 1 \quad \text{και} \quad \psi^* \circ \varphi^* = 1.$$

Από την προσεταιριστικότητα της σύνθεσης συναρτήσεων προκύπτει ότι $\varphi^* \circ \psi^* = (\psi \circ \varphi)^*$. Άρα $(\psi \circ \varphi)^* = 1_{k[C_f]}$ και $(\varphi \circ \psi)^* = 1_{k[C_g]}$. Από τη μοναδικότητα (και την προφανή σχέση $1^*_{C_f} = 1_{k[C_f]}$) προκύπτει $\psi \circ \varphi = 1_{C_g}$ και $\varphi \circ \psi = 1_{C_f}$. Άρα οι $C_f$ και $C_g$ είναι ισόμορφες. □

**2.3.3 Παράδειγμα** Η κυβική $C_f$, $f = y^2 - x^3$ δεν είναι ισόμορφη με την ευθεία. Πράγματι, αν $C_f \cong k \times \{0\}$, τότε $k[C_f] \cong k[t]$ από το προηγούμενο θεώρημα. Αλλά $k[C_f] = k[t^2, t^3]$ (Παράδειγμα 2.2.2 (iii)). Οι $k$ άλγεβρες $k[t]$ και $k[t^2, t^3]$ δεν είναι ισόμορφες (γιατί;).

Ένα φυσικό ερώτημα που τίθεται εδώ είναι να ταξινομηθούν οι καμπύλες με προσέγγιση ισομορφίας. Μέχρι σήμερα δυστυχώς δεν υπάρχει έστω και μερικώς ικανοποιητική απάντηση.

## 2.4 Θεώρημα του Bezout και Θεώρημα του Pascal

Στο $k^{n+1}-\{0\}$ ορίζουμε μια σχέση ισοδυναμίας $(x_0,...,x_n)\sim(y_0,...,y_n)$ αν υπάρχει $\lambda\in k-\{0\}$ με την ιδιότητα $x_i=\lambda y_i$ για κάθε $i$. Το σύνολο των κλάσεων ισοδυναμίας του $k^{n+1}-\{0\}$ συμβολίζεται με $\mathbb{P}_k^n$ και ονομάζεται *προβολικός χώρος*. Στην παράγραφο αυτή, θα ασχοληθούμε με το $\mathbb{P}_{\mathbb{R}}^2$. Τα σημεία του $\mathbb{P}_{\mathbb{R}}^2$ συμβολίζονται με τριάδες της μορφής $(x:y:z)$, δηλαδή η κλάση που περιέχει το σημείο $(x,y,z)\in k^3-\{0\}$ συμβολίζεται με $(x:y:z)$. Διαισθητικά, τα στοιχεία του $\mathbb{P}_{\mathbb{R}}^2$ είναι οι ευθείες του $\mathbb{R}^3$ που διέρχονται από το $(0,0,0)$.

Έστω $f\in k[x,y,z]$ ένα ομογενές πολυώνυμο βαθμού $d$. Αυτό σημαίνει ότι $f(\lambda x,\lambda y,\lambda z)=\lambda^d f(x,y,z)$ για κάθε $\lambda\in k$, και άρα το σημείο $(x,y,z)\in k^3$ είναι ρίζα του $f$ αν και μόνον αν το $(\lambda x,\lambda y,\lambda z)$ είναι ρίζα του $f$, όπου $\lambda\in k-\{0\}$. Έτσι μπορούμε να ορίσουμε $C_f\subseteq\mathbb{P}_k^2$, όπου $C_f=\{(x:y:z)\in\mathbb{P}_k^2\mid f(x,y,z)=0\}$. Το σύνολο $C_f$ ονομάζεται *προβολική καμπύλη*. Αν το $f$ έχει βαθμό 2 η $C_f$ ονομάζεται κωνική. Η ταξινόμηση των κωνικών είναι κομψή και έπεται από το Φασματικό Θεώρημα της Γραμμικής Άλγεβρας.

**2.4.1 Θεώρημα** *Με κατάλληλη εκλογή των αξόνων, το πολυώνυμο κάθε κωνικής στο $\mathbb{P}_{\mathbb{R}}^2$ έχει μια από τις παρακάτω μορφές*

*(i)* $x^2+y^2-z^2$ *(μη εκφυλισμένη κωνική)*

*(ii)* $x^2+y^2+z^2$ *(κενό σύνολο)*

*(iii)* $x^2+y^2$ *(ένα σημείο)*

*(iv)* $x^2-y^2$ *(δύο ευθείες)*

*(v)* $x^2 = 0$ *(μια διπλή ευθεία)*

**Απόδειξη.** Το πολυώνυμο κάθε κωνικής στο $\mathbb{P}^2_{\mathbb{R}}$ έχει από τον ορισμό τη μορφή

$$ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz .$$

Σ' αυτό αντιστοιχούμε τον $3\times 3$ πραγματικό συμμετρικό πίνακα.

$$\begin{bmatrix} a & d & e \\ d & b & f \\ e & f & c \end{bmatrix}.$$

Το Φασματικό Θεώρημα μας πληροφορεί ότι ο πίνακας αυτός είναι ορθομοναδιαία όμοιος με ένα διαγώνιο πίνακα. Συνεπώς το πολυώνυμο μιας κωνικής στο $\mathbb{P}^2_{\mathbb{R}}$ παίρνει (για κατάλληλη εκλογή αξόνων) τη μορφή $\lambda x^2 + \mu y^2 + \nu z^2$, όπου $\lambda, \mu, \nu \in \mathbb{R}$. Αν τώρα $\lambda \neq 0$, αντικαθιστούμε το $x$ με το $x/\sqrt{|\lambda|}$. Όμοια για τα $\mu$, $\nu$. Έτσι μπορούμε να υποθέσουμε ότι $\lambda, \mu, \nu \in \{\pm 1, 0\}$. Αλλάζοντας –αν είναι ανάγκη– το πρόσημο του πολυωνύμου $\lambda x^2 + \mu y^2 + \nu z^2$, φθάνουμε στις περιπτώσεις (i)–(v) του Θεωρήματος. □

Για λόγους σύγκρισης παραθέτουμε την ταξινόμηση των κωνικών στο (σύνηθες) επίπεδο $\mathbb{R}^2$ που είναι γνωστή από την Αναλυτική Γεωμετρία: Με κατάλληλη εκλογή των αξόνων, το πολυώνυμο μιας κωνικής στο επίπεδο $\mathbb{R}^2$ παίρνει μία από τις παρακάτω μορφές

| | |
|---|---|
| $\frac{x^2}{a^2} + \frac{y^2}{b^2} - 1$ | (έλλειψη) |
| $y = mx^2$ | (παραβολή) |
| $\frac{x^2}{a^2} - \frac{y^2}{b^2} - 1$ | (υπερβολή) |
| $x^2 + y^2$ | (σημείο) |
| $x$ | (ευθεία) |
| $x^2 + y^2 - 1$ | (κενό σύνολο) |
| $x^2 = -1$ | (κενό σύνολο) |

$xy = 0$ (δύο ευθείες)

$x(x-1)$ (δύο παράλληλες ευθείες)

$x^2 = 0$ (διπλή ευθεία).

Παρατηρήστε ότι στο προβολικό επίπεδο, η έλλειψη, η παραβολή και η υπερβολή παριστάνονται από την ίδια εξίσωση $x^2 + y^2 - z^2 = 0$.

Ως συνέπεια του προηγούμενου αποτελέσματος, θα αποδείξουμε τώρα μια ειδική περίπτωση του θεωρήματος του Bezout που στη συνέχεια θα χρησιμοποιήσουμε για να πάρουμε μια σύντομη και όμορφη απόδειξη του θεωρήματος του Pascal που οφείλεται στον Plücker.

**2.4.2 Πρόταση** *(Bezout–ειδική περίπτωση). Έστω $C \subseteq \mathbb{P}^2_{\mathbb{R}}$ μια μη εκφυλισμένη κωνική και $C' \subseteq \mathbb{P}^2_{\mathbb{R}}$ μια καμπύλη βαθμού d. Αν το $C$ δεν είναι υποσύνολο του $C'$, τότε η τομή $C \cap C'$ περιέχει το πολύ $2d$ σημεία.*

**Απόδειξη.** Η εξίσωση της μη εκφυλισμένης κωνικής είναι $x^2 + y^2 - z^2 = 0$ (Θεώρημα 2.4.1), η οποία γίνεται $y^2 = xz$ αν θέσουμε στη θέση των $x, y$ και $z$ αντίστοιχα τα $x - z$, $2y$ και $x + z$. Μια παραμετρικοποίηση της $y^2 = xz$ είναι

$$x \mapsto t_1^2, \quad y \mapsto t_1 t_2, \quad z \mapsto t_2^2.$$

Έστω τώρα $g$ το ομογενές πολυώνυμο βαθμού $d$ της $C'$. Η εξίσωση της τομής είναι συνεπώς

$$g(t_1^2, t_1, t_2, t_2^2) = 0.$$

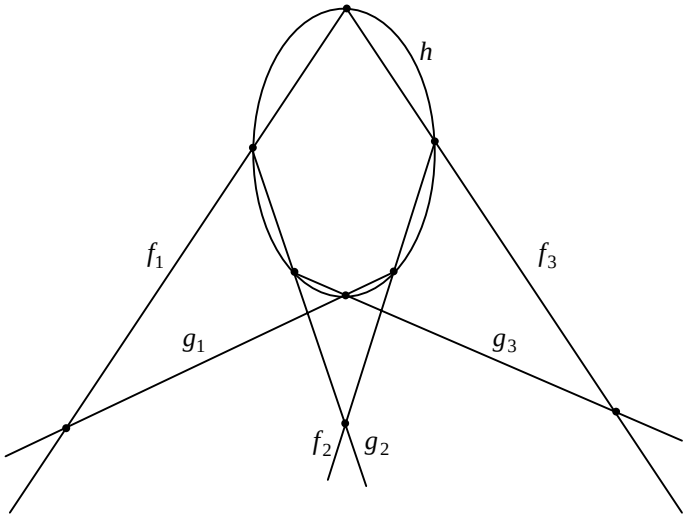
Όμως το πολυώνυμο $g(t_1^2, t_1, t_2, t_2^2)$ είναι μη μηδενικό (γιατί το $C$ δεν είναι υποσύνολο του $C'$) και ομογενές βαθμού $2d$. Ένα τέτοιο πολυώνυμο έχει το πολύ $2d$ ρίζες $(t_1 : t_2) \in \mathbb{P}^1_{\mathbb{R}}$. Πράγματι, έστω $f(x, y) = \sum_{i=0}^{m} a_i x^i y^{m-1}$ ένα ομογενές πολυώνυμο βαθμού $m$ και $(x_0 : y_0)$ μια ρίζα του στο $\mathbb{P}^1_{\mathbb{R}}$. Υποθέτοντας ότι $y_0 \neq 0$, έχουμε από $f(x_0, y_0) = 0$ τη σχέση

$$\sum_{i=0}^{m} (x_0 / y_0)^i = 0.$$

Άρα για το $x_0 / y_0$ υπάρχουν το πολύ $m$ δυνατότητες (γιατί είναι ρίζες πολυωνύμου μιας μεταβλητής βαθμού $m$). □

**2.4.3 Πόρισμα** *(Θεώρημα του Pascal). Έστω εξάγωνο εγγεγραμμένο σε μη εκφυλισμένη κωνική του* $\mathbb{P}^2_{\mathbb{R}}$. *Τότε οι απέναντι πλευρές του τέμνονται σε τρία συνευθειακά σημεία.*

**Απόδειξη.** *(Plücker)*




Ορίζουμε το πολυώνυμο τρίτου βαθμού $H_\lambda = f_1 f_2 f_3 + \lambda g_1 g_2 g_3$ όπου $\lambda \in \mathbb{R}$. Έστω $P$ ένα έβδομο σημείο πάνω στην κωνική διάφορο των έξι δεδομένων σημείων. Τότε $g_1 g_2 g_3(P) \neq 0$, αφού κάθε $g_i$ με την κωνική έχει το πολύ δύο κοινά σημεία. Άρα υπάρχει $\lambda_0 \in \mathbb{R}$, έτσι ώστε $H_{\lambda_0}(P) = 0$. Έχουμε

$$\# C_h \cap C_{H_{\lambda_0}} \geq 7 .$$

Επομένως η Πρόταση 2.4.2 δίνει $C_h \subseteq C_{H_{\lambda_0}} = C_h \cup \varepsilon$, όπου $\varepsilon$ είναι κάποια ευθεία. Έστω $P_i$ το σημείο $C_{f_i} \cap C_{g_i}$. Τότε $H_{\lambda_0}(P_i) = 0$. Επίσης $P_i \notin C_h$, γιατί μια μη

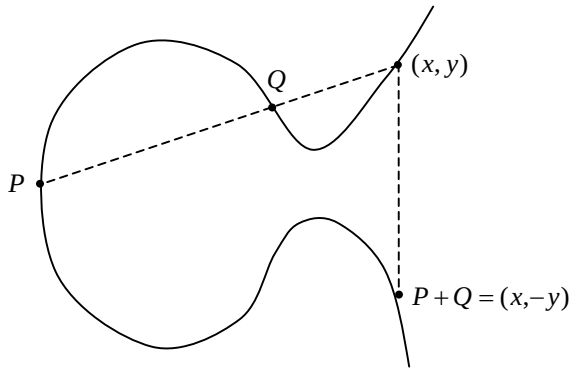
εκφυλισμένη κωνική δεν μπορεί να περιέχει τρία διάφορα συνευθειακά σημεία. Άρα $P_i \in \varepsilon$, δηλαδή τα $P_i$ είναι συνευθειακά. □

## 2.5 Κυβικές καμπύλες ως ομάδες

Στην παράγραφο αυτή θα δείξουμε πως σε μια κυβική καμπύλη (μη ιδιάζουσα) ορίζεται η δομή αβελιανής ομάδας. Στη συνέχεια θα διατυπώσουμε (χωρίς απόδειξη) μερικά σημαντικά θεωρήματα ενδεικτικά του βάθους του αντικειμένου.

Θεωρούμε μια κυβική καμπύλη $C \subseteq \mathbb{R}^2$ με εξίσωση της μορφής $y^2 = x^3 + ax + b$, όπου το πολυώνυμο $x^3 + ax + b$ δεν έχει διπλές ρίζες. Θα επισυνάψουμε στο σύνολο $C$ ένα σημείο, το "σημείο στο άπειρο", και θα δείξουμε ότι στο $C' = C \cup \{\infty\}$ ορίζεται με γεωμετρικό τρόπο δομή αβελιανής ομάδας.

Έστω $P, Q \in C$. Ορίζουμε $P + \infty = \infty + P = P$. Για να ορίσουμε το $P + Q$ θεωρούμε την ευθεία $PQ$. Αν αυτή τέμνει την καμπύλη $C$ σε ένα τρίτο σημείο $(x, y)$, ορίζουμε $P + Q = (x, -y)$. Αν αυτή δεν τέμνει την $C$, ορίζουμε $P + Q = \infty$. (Αν $P = Q$, ορίζουμε το $P + Q$ όπως πριν με τη διαφορά ότι θεωρούμε την εφαπτομένη στο $P$. Εδώ χρειάζεται η υπόθεση ότι το $x^3 + ax + b$ δεν έχει διπλές ρίζες).



Μπορεί να δειχτεί ότι το σύνολο $C'$ με την προηγούμενη πρόσθεση είναι αβελιανή ομάδα. Το μόνο αξίωμα που δεν είναι προφανές είναι η προσεταιριστικότητα. Θα δείξουμε ότι ισχύει.

Έστω λοιπόν $P,Q,R \in C'$. Αν κάποιο απ' αυτά είναι το $\infty$ η προσεταιριστικότητα προφανώς ισχύει. Έστω τώρα $P,Q,R \in C$. Θα προσδιορίσουμε τις συντεταγμένες του $P+Q$, όπου $P=(x_1,y_1)$ και $Q=(x_2,y_2)$ με $x_1 \neq x_2$. (Αν $x_1 = x_2$, τότε $P+Q=\infty$).

Η ευθεία $PQ$ έχει εξίσωση $y-y_1=\dfrac{y_2-y_1}{x_2-x_1}(x-x_1)$. Άρα η τομή της με την $C$ δίνεται από την

$$\left(y_1+\frac{y_2-y_1}{x_2-x_1}(x-x_1)\right)^2 = x^3+ax+b.$$

Δύο ρίζες της εξίσωσης αυτής είναι γνωστές, οι $x_1$ και $x_2$. Άρα η τρίτη ρίζα $x_3$, ικανοποιεί $x_1+x_2+x_3=\left(\dfrac{y_2-y_1}{x_2-x_1}\right)^2$. Έτσι βρίσκουμε

$$\begin{aligned} x_3 &= -x_1-x_2+\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 \\ y_3 &= y_1+\frac{y_2-y_1}{x_2-x_1}(x_3-x_1) \end{aligned} \tag{2}$$

Τότε $P+Q=(x_3,-y_3)$.

Με παρόμοιο τρόπο προσδιορίζουμε τις συντεταγμένες του $2P=(\alpha,\beta)$. Έχουμε

$$\begin{aligned} \alpha &= -2x_1+\left(\frac{3x_1^2+a}{2y_1}\right)^2, \\ \beta &= y_1+\frac{3x_1^2+a}{2y_1}(x_3-x_1). \end{aligned} \tag{3}$$

(Αν $y_1=0$, τότε $2P=\infty$). Τώρα η απόδειξη της προσεταιριστικότητας είναι μια (κουραστική) υπόθεση ρουτίνας αντικατάστασης των εξισώσεων (2) και (3), που φυσικά παραλείπεται.

Οι εξισώσεις (2) και (3) δείχνουν ότι τα ρητά σημεία της $C$ (μαζί βέβαια με το ουδέτερο στοιχείο $\infty$) αποτελούν μία υποομάδα της $C$. Ας τη συμβολίσουμε με $C(\mathbb{Q})$.

Ο Mordell απέδειξε το 1922 μια εικασία του Poicaré (1901) σύμφωνα με τον οποίο η αβελιανή ομάδα $C(\mathbb{Q})$ είναι πεπερασμένα παραγόμενη.

**2.5.1 Θεώρημα** *(Mordell, 1922). Η αβελιανή ομάδα* $C(\mathbb{Q})$ *είναι πεπερασμένα παραγόμενη.*

Λίγο αργότερα, ο Weil γενίκευσε το θεώρημα του Mordell για πεπερασμένες επεκτάσεις του $\mathbb{Q}$. Τέλος αναφέρουμε ότι ο Mazur απέδειξε ότι για την υποομάδα στρέψης της $C(\mathbb{Q})$ (δηλαδή την υποομάδα που σχηματίζουν τα στοιχεία πεπερασμένης τάξης) δεν υπάρχουν παρά μόνο ελάχιστες δυνατότητες.

**2.5.2 Θεώρημα** *(Mazur, 1976). Η υποομάδα στρέψης της* $C(\mathbb{Q})$ *είναι μία από τις ακόλουθες*

$$\mathbb{Z}_m, \quad m \le 10$$

$$\mathbb{Z}_{12}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}, \quad m \le 4.$$

Τα στοιχεία άπειρης τάξης της $C(\mathbb{Q})$ αποτελούν μία ελεύθερη αβελιανή ομάδα. Έστω $r = r_C$ η τάξη της. Υπάρχουν εδώ πολλά ανοικτά ερωτήματα όπως: υπάρχει $m \in \mathbb{N}$ έτσι ώστε $r_C < m$ για κάθε $C$; Μια φημισμένη εικασία στη Θεωρία Αριθμών συνδέει τον αριθμό $r$ με την τάξη του πόλου στο $\sigma = 1$ της αντίστοιχης $L$-συνάρτησης (εικασία Birch, Swinnerton-Dyer).

Για τα θεωρήματα και τις εικασίες που αναφέραμε πιο πάνω παραπέμπουμε στο βιβλίο των K. Ireland and M. Rosen που αναφέρεται στη Βιβλιογραφία.

## Ασκήσεις

**1.** Λύστε τις Διοφαντικές εξισώσεις

(i) $2x^2 + y^2 = 25z^2$, (ii) $3x^2 + y^2 = 11z^2$.

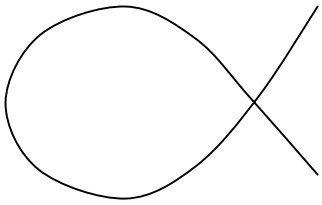
**2.** Ποιες από τις καμπύλες

$$y = x^5, \quad y^2 = x^5, \quad xy = 1, \quad x^2 + y^2 = 1$$

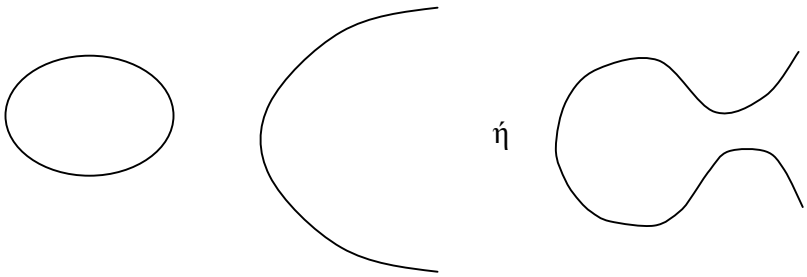
είναι ισόμοφρες με την ευθεία; Εδώ $k = \mathbb{C}$.

**3.** Κάθε κωνική καμπύλη $C \subseteq k^2$ είναι ρητή.

**4.** (i) Κάθε κυβική καμπύλη $C \subseteq k^2$ της μορφής $y^2 = x^3 + ax + b$, όπου το $x^3 + ax + b$ έχει πολλαπλή ρίζα, είναι ρητή (σχήμα). Εδώ $k = \mathbb{C}$.



(ii) Δώστε ένα παράδειγμα κυβικής της μορφής $y^2 = x^3 + ax + b$ που δεν είναι ρητή (σχήμα).




**5.** Η καμπύλη $(x^2 + y^2)^2 = a(x^2 - y^2)$ ("λημνίσκος") είναι ρητή. (Υπόδειξη: Θεωρήστε την τομή με τους κύκλους $x^2 + y^2 = t(x - y)$).

**6.** Ποια είναι τα στοιχεία τάξης 2 της ομάδας της κυβικής $y^2 = x^3 + ax + b$ (στο $\mathbb{R}^2$); Ποια είναι η υποομάδα που αυτά σχηματίζουν;

**7.** Έστω $C$ η κυβική που ορίζεται από $y^2 = x^3$. Αποδείξτε ότι στο $C$ ορίζεται η δομή Αβελιανής ομάδας με ουδέτερο στοιχείο το $0 = (0,0)$ τέτοια ώστε

$$P+Q+R=0 \Leftrightarrow P,Q,R \text{ είναι συνευθειακά.}$$

**8.** Έστω $k$ αλγεβρικά κλειστό σώμα και $f \in k[x,y]$ ανάγωγο. Ένα σημείο $(\alpha,\beta) \in C_f$ ονομάζεται *ιδιάζον* αν

$$f(\alpha,\beta)=\frac{\partial f}{\partial x}(\alpha,\beta)=\frac{\partial f}{\partial y}(\alpha,\beta)=0 .$$

Αποδείξετε ότι η $C_f$ έχει το πολύ πεπερασμένο πλήθος ιδιάζοντα σημεία. (Υπόδειξη: διακρίνετε περιπτώσεις ανάλογα αν η χαρακτηριστική του $k$ είναι $0$ ή $p>0$).

# Κεφάλαιο 3

# Πρότυπα

Στο κεφάλαιο αυτό εισαγάγουμε την έννοια του προτύπου πάνω από δακτύλιο που θα παίξει σημαντικό ρόλο στα επόμενα κεφάλαια. Η έννοια αυτή είναι αρκετά γενική – για παράδειγμα κάθε ιδεώδες $I$ του δακτυλίου $R$ και κάθε πηλίκο $R/I$ είναι πρότυπα πάνω από το $R$ – και κατέχει κεντρική θέση στη σύγχρονη Άλγεβρα.

## 3.1 Ορισμοί και Παραδείγματα

**3.1.1 Ορισμός** *Έστω $R$ ένας δακτύλιος. Μια Αβελιανή ομάδα $M$ εφοδιασμένη με μια απεικόνιση*

$$R \times M : (r, m) \mapsto r \cdot m \in M$$

*ονομάζεται $R$- πρότυπο ή πρότυπο πάνω από το $R$ αν ισχύουν*

*(i)* $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$ *για κάθε* $r_1, r_2 \in R$, $m \in M$

*(ii)* $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$ *για κάθε* $r_1, r_2 \in R$, $m \in M$

*(iii)* $r \cdot (m_1 + m_2) \cdot = r \cdot m_1 + r \cdot m_2$ *για κάθε* $r \in R$, $m_1, m_2 \in M$

*(iv)* $1_R \cdot m = m$ *για κάθε* $m \in M$ .

Στα παρακάτω θα γράφουμε $rm$ στη θέση του $r \cdot m$ . Στον προηγούμενο ορισμό, θα ονομάζουμε την απεικόνιση $R \times M \to M$ , τον "εξωτερικό πολλαπλασιασμό" του $M$.

**3.1.2 Παράδειγμα** (i) Κάθε $k$ - διανυσματικός χώρος, όπου το $k$ είναι σώμα, είναι $k$ – πρότυπο. Μάλιστα οι έννοιες $k$ - διανυσματικός χώρος και $k$ – πρότυπο ταυτίζονται όταν το $k$ είναι σώμα, όπως φαίνεται από τη σύγκριση των παραπάνω αξιωμάτων με αυτά στον ορισμό του διανυσματικού χώρου.

(ii) Κάθε Αβελιανή ομάδα $M$ είναι $\mathbb{Z}$ - πρότυπο με εξωτερικό πολλαπλασιασμό που ορίζεται από τη σχέση

$$rm = \begin{cases} m+...+m \ (r \text{ φορές}), & \text{αν } r > 0 \\ 0, & \text{αν } r = 0 \\ (-r)m, & \text{αν } r < 0, \end{cases}$$

όπου $r \in \mathbb{Z}$ και $m \in M$.

(iii) Κάθε ιδεώδες $I$ του $R$ είναι $R$ – πρότυπο με εξωτερικό πολλαπλασιασμό το πολλαπλασιασμό στοιχείων του $R$.

(iv) Έστω $I$ ένα ιδεώδες του δακτυλίου $R$. Ο δακτύλιος $R/I$ είναι ένα $R$ – πρότυπο με εξωτερικό πολλαπλασιασμό που ορίζεται από τη σχέση

$$r(a+I) = ra + I,$$

όπου $r \in R$ και $a + I \in R/I$. Η σχέση αυτή είναι καλά ορισμένη, γιατί αν $a + I = a' + I$, τότε $a - a' \in I$ και άρα $r(a-a') \in I$ που σημαίνει ότι $ra + I = ra' + I$. Η επαλήθευση τώρα των αξιωμάτων του ορισμού 3.1.1 είναι θέμα ρουτίνας.

(v) Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων. Τότε ο $S$ είναι $R$ – πρότυπο με εξωτερικό πολλαπλασιασμό που ορίζεται από τη σχέση

$$rs = \varphi(r)s$$

Ας επαληθεύσουμε ενδεικτικά το αξίωμα (ii) του ορισμού. Έχουμε $(r_1 + r_2)s = \varphi(r_1 + r_2)s = (\varphi(r_1) + \varphi(r_2))s = \varphi(r_1)s + \varphi(r_2)s = r_1 s + r_2 s$.

**3.1.3 Παρατήρηση** *Έστω $M$ ένα $R$ – πρότυπο. Τότε έχουμε*

*(i)* $0_R m = 0_M$ *για κάθε* $m \in M$

*(ii)* $r0_M = 0_M$ *για κάθε* $r \in R$

*(iii)* $(-r)m = r(-m) = -rm$ *για κάθε* $r \in R$, $m \in M$

**Απόδειξη.** (i) Έχουμε $0_R + 0_R = 0_R \Rightarrow (0_R + 0_R)m = 0_R m \Rightarrow 0_R m + 0_R m = 0_R m$ από το αξίωμα (ii) του Ορισμού 3.1.1. Άρα $0_R m + 0_R m = 0_R m + 0_M$. Από το νόμο της διαγραφής που ισχύει στην ομάδα $M$ παίρνουμε $0_R m + 0_M$.

(ii) Έχουμε: $0_M + 0_M = 0_M \Rightarrow r(0_M + 0_M) = r0_M \Rightarrow r0_M + r0_M = r0_M$ από το αξίωμα (iii) του ορισμού 3.1.1. Όπως και πριν παίρνουμε $r0_m = 0_m$.

(iii) $r(m+(-m)) = r0_M = 0_M$ από το (ii). Συνεπώς $rm + r(m) = 0_m$ και άρα $r(-m) = -(rm)$. Όμοια $(r+(-r))m = 0_R = 0_M$ από το (i). Συνεπώς $rm + (-r)m = 0_M$. Άρα $(-r)m = -(rm)$. □

Στο παρακάτω θα χρησιμοποιήσουμε τις σχέσεις της Παρατήρησης 3.1.3 χωρίς ιδιαίτερη μνεία. Αξίζει να σημειωθεί ότι σ' ένα $R$ – πρότυπο $M$ είναι δυνατό να ισχύει $rm = 0$ με $r \neq 0_R$ και $m \neq 0_M$. Για παράδειγμα, στο $\mathbb{Z}$ - πρότυπο $\mathbb{Z}_n$ ισχύει $n[a] = [na] = [0]$ για κάθε $[a] \in \mathbb{Z}_n$.

**3.1.4 Ορισμός** *Έστω $M$ ένα $R$ – πρότυπο. Ένα υποσύνολο $N \subseteq M$ ονομάζεται $R$ – υποπρότυπο του $M$ αν το $N$ είναι $R$ – πρότυπο ως προς την πρόσθεση και τον εξωτερικό πολλαπλασιασμό του $M$. Στην περίπτωση αυτή χρησιμοποιούμε το συμβολισμό $N \leq M$.*

**3.1.5 Λήμμα** *Έστω $M$ ένα $R$ – πρότυπο και $N \subseteq M$ ένα μη κενό υποσύνολο του $M$. Τότε το $N$ είναι υποπρότυπο του $M$ αν και μόνο αν*

*(i)* $a, b \in N \Rightarrow a - b \in N$

*(ii)* $a \in N, r \in R \Rightarrow ra \in N$

**Απόδειξη.** Έστω $N \leq M$. Τότε το $N$ είναι υποομάδα του $M$ και συνεπώς ισχύει η (i). Η συνθήκη (ii) έπεται άμεσα από τον Ορισμό 3.1.4. Αντίστροφα, έστω ότι ισχύουν οι (i), (ii). Από την (i) συμπεραίνουμε ότι το $N$ είναι υποομάδα του $M$. Επειδή τώρα ισχύει η (ii), θα ισχύουν όλα τα αξιώματα του Ορισμού 3.1.1 για το $N$. □

**3.1.6 Παράδειγμα** (i) Έστω $R$ ένας δακτύλιος. Τα $R$ – υποπρότυπα του $R$ είναι ακριβώς τα ιδεώδη του $R$.

(ii) Τα $\mathbb{Z}$ - υποπρότυπα μιας Αβελιανής ομάδας είναι ακριβώς οι υποομάδες της.

(iii) Έστω $k$ σώμα. Τα $k$- υποπρότυπα ενός $k$ – διανυσματικού χώρου είναι ακριβώς οι υπόχωροί του.

Από το Λήμμα 3.1.5 έπεται άμεσα ότι η τομή μιας (μη κενής) οικογένειας $R$-υποπροτύπων ενός $R$-προτύπου είναι πάλι ένα $R$-πρότυπο. Αυτό μας οδηγεί στον επόμενο ορισμό.

**3.1.7 Ορισμός** *Έστω $X \neq \varnothing$ ένα υποσύνολο του $R$-προτύπου $M$. Το υποπρότυπο του $M$ που παράγεται από το $X$ είναι η τομή όλων των υποπροτύπων του $M$ που περιέχουν το $X$. Αυτό συμβολίζεται με $\langle X \rangle$.*

**3.1.8 Πρόταση** *Έστω $X \neq \varnothing$ ένα υποσύνολο του $R-$προτύπου $M$.*
*Τότε*

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N},\ r_i \in R,\ x_i \in X \right\}.$$

**Απόδειξη.** Έστω $A$ το δεξί μέλος της παραπάνω ισότητας. Ισχύει $A \subseteq \langle X \rangle$. Πράγματι, έστω $N$ ένα υποπρότυπο του $M$ που περιέχει το $X$. Τότε $x_i \in X \Rightarrow x_i \in N \Rightarrow r_i x_i \in N$. Άρα $\sum_{i=1}^{n} r_i x_i \in N$. Συνεπώς $\sum_{i=1}^{n} r_i x_i \in \langle X \rangle$. Ισχύει $\langle X \rangle \subseteq A$. Πράγματι το $A$ είναι υποπρότυπο του $M$ (όπως συμπεραίνουμε από το Λήμμα 3.1.5) που περιέχει το $X$. Το $\langle X \rangle$ ως τομή τέτοιων προτύπων θα περιέχεται στο $A$.

□

Αν το $X$ είναι πεπερασμένο, $X = \{x_1, ..., x_m\}$, θα συμβολίζουμε το $\langle X \rangle$ με $\langle x_1, ..., x_n \rangle$ ή $Rx_1 + ... + Rx_n$ και θα λέμε ότι το $\langle X \rangle$ παράγεται από τα $x_1, ..., x_n$.

**3.1.9 Ορισμός** *(i) Ένα $R$-πρότυπο $M$ λέγεται πεπερασμένα παραγόμενο αν υπάρχει πεπερασμένο υποσύνολο $X \subseteq M$ με την ιδιότητα $\langle X \rangle = M$.*

*(ii) Ένα $R$-πρότυπο $M$ λέγεται κυκλικό αν παράγεται από κάποιο $a \in M$, δηλαδή αν $M = \langle a \rangle$.*

Για παράδειγμα τα κυκλικά $k-$υποπρότυπα ενός $k-$διανυσματικού χώρου ($k$ σώμα) είναι οι υπόχωροι διάστασης 1 και ο τετριμμένος υπόχωρος.

**Σχόλιο.** Όλοι οι προηγούμενοι ορισμοί γενικεύουν κατά τρόπο προφανή αντίστοιχες έννοιες της Γραμμικής Άλγεβρας. Το ίδιο θα συμβεί στην επόμενη παράγραφο. Ας μη θεωρηθεί όμως ότι η θεωρία προτύπων είναι απλοϊκή γενίκευση της Γραμμικής Άλγεβρας! Η δομή $R$-προτύπων δεν συγκρίνεται ως προς την πολυπλοκότητα και το μαθηματικό ενδιαφέρον με τη δομή $k$-διανυσματικών χώρων. Αυτό θα γίνει φανερό στην Παράγραφο 3.4, όταν θα μελετήσουμε ελεύθερα πρότυπα.

## 3.2 Ορισμοί και Παραδείγματα

**3.2.1 Ορισμός** *Έστω $M$ και $N$ δύο $R$-πρότυπα. Μία απεικόνιση $\varphi : M \to N$ ονομάζεται ομομορφισμός $R$-προτύπων (ή $R$-γραμμική) αν:*

*(i)* $\varphi(m+m') = \varphi(m) + \varphi(m')$ *για κάθε* $m, m' \in M$ *, και*

*(ii)* $\varphi(rm) = r\varphi(m)$ *για κάθε* $r \in R,\ m \in M$ .

Ένας ομομορφισμός $R$-προτύπων $\varphi : M \to N$ ονομάζεται *επιμορφισμός* (αντίστοιχα *μονομορφισμός*) αν ως απεικόνιση η $\varphi$ είναι επί (αντίστοιχο αμφιμονοσήμαντη). Ισομορφισμός $R$-προτύπων είναι ένας ομομορφισμός που είναι ταυτόχρονα ως απεικόνιση επί και αμφιμονοσήμαντη. Συμβολισμός: για $R$-πρότυπα $M$ και $N$, γράφουμε $M \triangleright N$ όταν υπάρχει ισομορφισμός $M \to N$ . Τότε αυτά λέγονται ισόμορφα.

**3.2.2 Παράδειγμα** (i) Αν $M$ και $N$ είναι $R$-πρότυπα η μηδενική απεικόνιση $M \ni m \mapsto 0 \in N$ είναι ομομορφισμός $R$-προτύπων. Η ταυτοτική απεικόνιση $1_M : M \ni m \mapsto m \in M$ είναι επίσης ομομορφισμός $R$-προτύπων.

(ii) Αν $V$ και $W$ είναι $k$ – διανυσματικοί χώροι ($k$ σώμα), οι ομομορφισμοί $k$ – προτύπων $V \to W$ είναι ακριβώς οι $k$-γραμμικές απεικονίσεις $V \to W$ .

(iii) Αν $G$ και $H$ είναι δύο Αβελιανές ομάδες, οι ομομορφισμοί $\mathbb{Z}$ -προτόπων $G \to H$ είναι ακριβώς οι ομομορφισμοί ομάδων $G \to H$ .

(iv) Έστω $R$ δακτύλιος και $a \in R$ . Η απεικόνιση $R \in x \mapsto ax \in R$ είναι ομομορφισμός $R$-προτύπων αλλά όχι γενικά ομομορφισμός δακτυλίων (γιατί;).

Έστω $\varphi : M \to N$ ομομορφισμός $R$-προτύπων. Ο πυρήνας

$$\ker \varphi = \{a \in M \mid \varphi(a) = 0\}$$

είναι Αβελιανή ομάδα (γιατί ο $\varphi$ είναι ομομορφισμός Αβελιανών ομάδων). Επιπλέον είναι *R*-υποπρότυπο του *M* γιατί $a \in \ker\varphi \Rightarrow \varphi(a) = 0 \Rightarrow r\varphi(a) = 0 \Rightarrow \varphi(ra) = 0 \Rightarrow ra \in \ker\varphi$. Κατά παρόμοιο τρόπο, η εικόνα του $\varphi$ είναι *R*-υποπρότυπο του *N*.

**3.2.3 Πρόταση** *Έστω* $\varphi : M \to N$ *ομομορφισμός R-προτύπων. Τότε ο* $\varphi$ *είναι μονομορφισμός αν και μόνο αν* $\ker\varphi = \{0\}$.

**Απόδειξη.** Όμοια με την Πρόταση 0.3.1. □

Έστω *M* ένα *R*-πρότυπο και $N \le M$. Θεωρώντας αυτά ως Αβελιανές ομάδες, ορίζεται στο πηλίκο $M/N = \{a + N \mid a \in M\}$ δομή Αβελιανής ομάδας με πρόσθεση $(a+N)+(b+M) = (a+b)+N$. Επιπλέον τώρα ορίζουμε δομή $R$ – προτύπου θέτοντας $r(a+N) = ra + N$. Εύκολα αποδείχνεται ότι η σχέση αυτή είναι καλά ορισμένη. Πράγματι έχουμε

$a + N = a' + N \Rightarrow a - a' \in N \Rightarrow r(a-a) = ra - ra' \in N \Rightarrow ra + N = ra' \in N$.

Η επαλήθευση των αξιωμάτων του Ορισμού 3.1.1 είναι άμεση.

Κατ' αναλογία με τους διανυσματικούς χώρους, τις αβελιανές ομάδες και τα ιδεώδη, υπάρχουν και εδώ θεωρήματα ισομορφισμών. Έστω *M* ένα *R*-πρότυπο και *A*, *B* υποπρότυπα του *M*. Με $A + B$ συμβολίζουμε το υποπρότυπο του *M* που παράγεται από το υποσύνολο $A \cup B$ (Ορισμός 3.1.7). Φυσικά ισχύει $A + B = \{a + b \in M \mid a \in A, b \in B\}$.

**3.2.4 Θεώρημα**

*1ο Θεώρημα Ισομορφισμών Προτύπων: Έστω* $\varphi : M \to N$ *ένας ομομορφισμός R-προτύπων. Τότε η απεικόνιση*

$$\overline{\varphi} : M/N \ni m + N \mapsto \varphi(m) \in \operatorname{Im}\varphi$$

*είναι ισομορφισμός R-προτύπων.*

*2ο Θεώρημα Ισομορφισμών Προτύπων: Έστω ότι* $A, B$ *είναι R-υποπρότυπα του R-προτύπου* $M$. *Τότε υπάρχει ισομορφισμός R-προτύπων*

$$(A+B)/A \simeq B/A \cap B.$$

*3ο Θεώρημα Ισομορφισμών Προτύπων: Έστω* $A \supseteq B \supseteq C$ *R-πρότυπα. Τότε υπάρχει ισομορφισμός R-προτύπων*

$$(A/C)/(B/C) \simeq A/B.$$

**Απόδειξη.**

1) Όμοια με την απόδειξη του θεωρήματος 0.3.2.

2) Η απεικόνιση

$$\varphi : B \to (A+B)/A,\ \varphi(b) = b + A$$

είναι επιμορφισμός $R$-προτύπων. Ισχύει $\ker\varphi = \{b \in B \mid b + A = 0\} = A \cap B$. Άρα από το 1ο Θεώρημα Ισομορφισμών Προτύπων προκύπτει $B/A \cap B \simeq (A+B)/A$.

3) Εφόσον $C \subseteq B$ η απεικόνιση

$$\varphi : A/C \to A/B,\ \varphi(a + C) = a + B$$

είναι ένας καλά οριζόμενος επιμορφισμός $R$-προτύπων. Ισχύει $\ker\varphi = \{a + C \mid a + B = B\} = B/C$. Άρα από το 1ο Θεώρημα Ισομορφισμών $R$-προτύπων προκύπτει $(A/C)/(B/C) \simeq A/B$. □

Ίσως είναι η κατάλληλη στιγμή να εισάγουμε την πρώτη έννοια που ανάλογή στους διανυσματικούς χώρους δεν υπάρχει (ακριβέστερη είναι τετριμμένη). Έστω $M$ ένα $R$-πρότυπο. Το σύνολο $\operatorname{Ann} M = \{r \in R \mid ra = 0$ για κάθε $a \in M\}$ είναι ιδεώδες του $R$. Πράγματι, (i) $\operatorname{Ann} M \neq \varnothing$ αφού $0 \in \operatorname{Ann} M$, (ii) $r, s \in A\operatorname{Ann} M \Rightarrow (r+s)a = ra + sa = 0$ για κάθε $a \in M$ και άρα $r + s \in \operatorname{Ann} M$, και (iii) $x \in R$, $r \in \operatorname{Ann} M \Rightarrow (xr)a = x(ra) = 0$ για κάθε $a \in M$ και άρα $xr \in \operatorname{Ann} M$. Το ιδεώδες $\operatorname{Ann} M$ ονομάζεται μηδενιστής του $M$. Για διανυσματικούς χώρους ισχύει βέβαια $\operatorname{Ann} V = (0)$. Για το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_m$ ισχύει $\operatorname{Ann}\mathbb{Z}_m = (m)$.

Αν $M$ και $N$ είναι δύο $R$-πρότυπα τότε το ευθύ γινόμενό τους $M \times N$ είναι το σύνολο $M \times N = \{(x, y) \mid x \in M, y \in N\}$ με πρόσθεση και εξωτερικό πολλαπλασιασμό που ορίζονται από τις σχέσεις

$$(x, y) + (x' + y') = (x + x', y + y')$$

$$r(x, y) = (rx, ry),$$

όπου $x, x' \in M$, $y, yx \in N$ και $r \in R$. Το $M \times N$ είναι ένα $R$-πρότυπο. Πιο γενικά αν $(M_\lambda)_{\lambda\in\Lambda}$ είναι μια οικογένεια $R$-προτύπων, τότε το σύνολο των ακολουθιών

$(x_\lambda)_{\lambda\in\Lambda}$ με $x_\lambda \in M_\lambda$, είναι ένα *R*-πρότυπο με πρόσθεση και εξωτερικό πολλαπλασιασμό που ορίζονται από τις σχέσεις $(x_\lambda)_{\lambda\in\Lambda} + (x'_\lambda)_{\lambda\in\Lambda} = (x_\lambda + x'_\lambda)_{\lambda\in\Lambda}$, $r(x_\lambda)_{\lambda\in\Lambda} = (rx_\lambda)_{\lambda\in\Lambda}$. Θα το συμβολίζουμε με $\prod_{\lambda\in\Lambda} M_\lambda$. Κατασκευάζουμε τώρα ένα *R*-υποπρότυπο του $\prod_{\lambda\in\Lambda} M_\lambda$. Έστω $\bigoplus_{\lambda\in\Lambda} M_\lambda$ το υποσύνολο του $\prod_{\lambda\in\Lambda} M_\lambda$ που αποτελείται από τις ακολουθίες $(x_\lambda)_{\lambda\in\Lambda}$ όπου $x_\lambda = 0_{M_\lambda}$ για κάθε $\lambda \in \Lambda$ εκτός το πολύ ένα πεπερασμένο πλήθος. Εύκολα επαληθεύεται ότι αυτό είναι ένα υποπρότυπο του $\prod_{\lambda\in\Lambda} M_\lambda$ και ονομάζεται *ευθύ άθροισμα* των $M_\lambda$. Στην ειδική αυτή περίπτωση που το *Λ* είναι πεπερασμένο σύνολο, έχουμε $\prod_{\lambda\in\Lambda} M_\lambda = \bigoplus_{\lambda\in\Lambda} M_\lambda$.

Έστω $(N_\lambda)_{\lambda\in\Lambda}$ μια οικογένεια *R*-υποπροτύπων του *R*-προτύπου *M*. Θα λέμε ότι το *M* είναι το *εσωτερικό ευθύ άθροισμα* των $N_\lambda$ αν κάθε $x \in M$ γράφεται κατά μοναδικό τρόπο ως άθροισμα της μορφής $x = y_{\lambda_1} + \cdots + y_{\lambda_t}$, με $y_{\lambda_i} \in N_{\lambda_i}$, $t \geq 1$. Στην περίπτωση αυτή θα γράφουμε $M = \bigoplus_{\lambda\in\Lambda} N_\lambda$.

**Σημείωση.** Η χρήση του συμβόλου $\bigoplus_{\lambda\in\Lambda} M_\lambda$ για δύο διαφορετικά πράγματα δεν πρέπει να δημιουργεί σύγχυση για τον εξής λόγο: αν $M = \bigoplus_{\lambda\in\Lambda} N_\lambda$ είναι το εσωτερικό ευθύ άθροισμα των υποπροτύπων $N_\lambda$, τότε το *M* είναι ισόμορφο με το ευθύ άθροισμα των προτύπων $N_\lambda, \lambda \in \Lambda$ (άσκηση).

Αν $(N_\lambda)_{\lambda\in\Lambda}$ είναι μια οικογένεια *R*-υποπροτύπων του *R*-προτύπου *M*, με $\sum_{\lambda\in\Lambda} N_\lambda$ συμβολίζουμε το *R*-υποπρότυπο του *M* που παράγεται από το σύνολο $\bigcup_{\lambda\in\Lambda} N_\lambda$.

**3.2.5 Πρόταση** *Έστω $(N_\lambda)_{\lambda\in\Lambda}$ μια οικογένεια R-υποπροτύπων του R-προτύπου M. Τότε ισχύει $M = \bigoplus_{\lambda\in\Lambda} N_\lambda$ αν και μόνο αν*

*(i)* $M = \sum_{\lambda\in\Lambda} N_\lambda$

*(ii)* *για κάθε* $\lambda \in \Lambda$ *ισχύει*

$$N_\lambda \cap \sum_{\substack{\mu\in\Lambda\\ \mu\neq\lambda}} N_\mu = 0$$

**Απόδειξη.** Αν $x \in M$ και $x = y_{\lambda_1} + ... + y_{\lambda_t} = y'_{\lambda_1} + ... + y'_{\lambda_t}$ με $y_{\lambda_i} y'_{\lambda_i} \in N_{\lambda_i}$ τότε

$$N_{\lambda_1} \ni y_{\lambda_1} - y'_{\lambda_1} = (y'_{\lambda_2} - y_{\lambda_2}) + ... + (y'_{\lambda_t} - y_{\lambda t}) \in \sum_{\substack{\mu\in\Lambda\\ \mu\neq\lambda_1}} N_\mu .$$

Τώρα αν ισχύει η συνθήκη (ii) παίρνουμε $y_{\lambda_1} = y'_{\lambda_1}$. Συνεπώς, αν ισχύουν οι συνθήκες της πρότασης, έχουμε $M = \bigoplus_{\lambda\in\Lambda} N_\lambda$. Αντίστροφα, αν κάθε $x \in M$ έχει μοναδική γραφή της μορφής $x = y_{\lambda_1} + ... + y_{\lambda_t}$, $y_{\lambda_i} \in N_{\lambda_i}$, τότε ισχύει προφανώς η συνθήκη (i). Αλλά και η συνθήκη (ii) ισχύει, γιατί αν $N_\mu \cap \sum_{\substack{\lambda\in\Lambda\\ \lambda\neq\mu}} N_\lambda \neq 0$ θα είχαμε $y_\mu = y_{\lambda_1} + ... + y_{\lambda_t}$ με $y_{\lambda_i} \in N_{\lambda_i}$, $\lambda_i \neq \mu$, δηλαδή θα είχαμε δύο εκφράσεις για το $y_\mu$. □

## 3.3 Ακριβείς Ακολουθίες

Έστω $\alpha : L \to M$, $\beta : M \to N$ ομομορφοφισμοί R-προτύπων. Η ακολουθία

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N$$

ονομάζεται *ακριβής* στο $M$ αν ισχύει $\mathrm{Im}\,\alpha = \ker\beta$.

Πιο γενικά μια ακολουθία $R$-προτύπων και $R$-ομομορφισμών

$$\cdots \to M_{i+1} \xrightarrow{\alpha_{i+1}} M_i \xrightarrow{\alpha_i} M_{i-1} \to \cdots$$

ονομάζεται *ακριβής* αν είναι ακριβής σε κάθε $M$.

Μια ακριβής ακολουθία της μορφής

$$0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$$

ονομάζεται *βραχεία ακριβής ακολουθία*. Στην περίπτωση αυτή ισχύουν (i) $\alpha$ είναι μονομορφισμός αφού $\ker\alpha = (0)$, (ii) $\ker\beta = \mathrm{Im}\,\alpha$, (iii) $\beta$ είναι επιμορφισμός

αφού $\mathrm{Im}\,\beta = \ker(M_3 \to 0) = M_3$. Αντίστροφα, αν η (*) ικανοποιεί τις (i), (ii) και (iii) τότε είναι ακριβής ακολουθία.

Αν $M_1 \xrightarrow{\alpha} M_2$ είναι μονομορφισμός $R$-προτύπων, τότε ορίζεται μια βραχεία ακριβής ακολουθία

$$0 \to M_1 \xrightarrow{\alpha} M_2 \to M_2 / \mathrm{Im}\,\alpha \to 0$$

όπου $M_2 \to M_2 / \mathrm{Im}\,\alpha$ είναι φυσική προβολή:

$$M_2 \ni x \mapsto x + \mathrm{Im}\,\alpha \in M_2 / \mathrm{Im}\,\alpha\,.$$

Από την άλλη μεριά, αν η (*) είναι ακριβής τότε υπάρχει ισομορφισμός $R$-προτύπων, $M_3 \simeq M_2 / \mathrm{Im}\,\alpha$. Αυτό ισχύει, γιατί $\mathrm{Im}\,\alpha = \ker\beta$ και $M_2 / \ker\beta \simeq \mathrm{Im}\,\beta = M_3$ από το 1ο Θεώρημα ισομορφισμών προτύπων.

**3.3.1 Πρόταση** *Έστω*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

*μια βραχεία ακριβής ακολουθία $R$-προτύπων. Τότε οι παρακάτω συνθήκες είναι ισοδύναμες*

*(i) υπάρχει $R$-ομομορφισμός $\alpha' : B \to A$ με την ιδιότητα $\alpha' \circ \alpha = 1_A$*

*(ii) υπάρχει $R$-ομομορφισμός $\beta' : C \to B$ με την ιδιότητα $\beta \circ \beta' = 1_B$*

*(iii) η εικόνα $\mathrm{Im}\,\alpha$ είναι ευθύς προσθετέος του $B$.*

**Απόδειξη.** (i) $\Rightarrow$(iii). Θα δείξουμε ότι $B = \mathrm{Im}\,\alpha + \ker\alpha'$ και $\mathrm{Im}\,\alpha \cap \ker\alpha' = 0$. Τότε θα ισχύει $B = \mathrm{Im}\,\alpha \oplus \ker\alpha'$ (Πρόταση 3.2.5). Γράφουμε

$$\beta = \alpha \circ \alpha'(b) + (b - \alpha \circ \alpha'(b))$$

Προφανώς $\alpha \circ \alpha'(b) \in \mathrm{Im}\,\alpha$. Επίσης $\alpha'(b - \alpha \circ \alpha'(b)) = \alpha'(b) - \alpha' \circ \alpha \circ \alpha'(b) = \alpha'(b) - \alpha'(b) = 0$. Άρα $B = \mathrm{Im}\,\alpha + \ker\alpha'$. Έστω $x \in \mathrm{Im}\,\alpha \cap \ker\alpha'$. Τότε $\alpha'(x) = 0$. Αλλά $x = \alpha(y)$ για κάποιο $y \in A$. Συνεπώς $\alpha'(\alpha(y)) = 0$ δηλαδή $y = 0$ οπότε $x = 0$. Συνεπώς $B = \mathrm{Im}\,\alpha \oplus \ker\alpha'$.

(ii) $\Rightarrow$(i) Έστω $B = \mathrm{Im}\,\alpha \oplus N$ για κάποιο υποπρότυπο $N$ του $B$. Έστω $b \in B$. Τότε $b = \alpha(x) + y$ για κάθε $x \in A$ και $y \in N$. Μάλιστα τα $x$ και $y$ είναι μοναδικά ορισμένα γιατί ο $\alpha$ είναι μονομορφισμός και $\mathrm{Im}\,\alpha \cap N = (0)$. Ορίζουμε $\alpha'(b) = x$.

Έτσι $\alpha' : B \to A$ είναι ένας καλά ορισμένος $R$-ομομορφισμός. Προφανώς $\alpha' \circ \alpha = 1_A$.

(ii) $\Rightarrow$(iii). Θα δείξουμε ότι $B = \ker\beta \oplus \mathrm{Im}\,\beta'$ απ' όπου προκύπτει το ζητούμενο γιατί $\ker\beta = \mathrm{Im}\,\alpha$. Έστω $b \in B$. Γράφουμε

$$b = (b - \beta' \circ \beta(b)) + \beta' \circ \beta(b)$$

και παρατηρούμε ότι $b - \beta' \circ \beta(b) \in \ker\beta$, αφού $\beta(b - \beta \circ \beta(b)) = \beta(b) - \beta(b) = 0$, και $\beta' \circ \beta(b) \in \mathrm{Im}\,\beta'$ προφανώς. Αν $x \in \ker\beta \cap \mathrm{Im}\,\beta'$, τότε $\beta(x) = 0$ και αφού $x = \beta'(y)$ για κάποιο $y \in C$, έχουμε $\beta' \circ \beta(y) = 0$ δηλαδή $y = 0$.

(iii) $\Rightarrow$(ii). Έστω $B = \mathrm{Im}\,\alpha \oplus N$ για κάποιο υποπρότυπο $N$ του $B$. Άρα $B = \ker\beta \oplus N$. Ο περιορισμός του $\beta$ στο $N$ $\beta_N : N \to C$ είναι ισομορφισμός. Πράγματι, αφού $B = \ker\beta + N$, ο $\beta_N$ είναι επί. Αν $\beta_N(y) = 0$ για κάποιο $y \in N$, τότε $y \in \ker\beta$ και άρα $y = 0$ αφού $\ker\beta \cap N = (0)$. Θέτοντας $\beta' = \beta_N^{-1}$ έχουμε το ζητούμενο. □

Μία βραχεία ακριβής ακολουθία που ικανοποιεί μία (και άρα όλες) από τις συνθήκες της προηγούμενης πρότασης λέγεται *διασπώμενη*. (Συχνά θα λέμε ότι η βραχεία ακριβής ακολουθία *διασπάται*).

Στην περίπτωση που η ακριβής ακολουθία

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

διασπάται ισχύει $B \simeq A \oplus C$. Πράγματι, από την απόδειξη της Πρότασης 3.3.1 έχουμε

$$B = \ker\beta \oplus \mathrm{Im}\,\beta'.$$

Αφού οι $\alpha$ και $\beta'$ είναι μονομορφισμοί (για το $\beta'$ ισχύει $\beta \circ \beta' = 1_c$) έχουμε $A \simeq \mathrm{Im}\,\alpha = \ker\beta$ και $\mathrm{Im}\,\beta' \simeq C$.

Αντίστροφα αν για $R$-πρότυπα ισχύει $B = A \oplus C$, τότε ορίζεται μια βραχεία ακριβής ακολουθία

$$0 \to A \xrightarrow{i} A \oplus C \xrightarrow{\pi} C \to 0,$$

όπου $i(a) = (a,0)$ και $\pi(a,c) = c$, που διασπάται.

**3.4.2 Παράδειγμα** 1) Η ακριβής ακολουθία $\mathbb{Z}$-προτύπων

$$0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}_2 \to 0,$$

όπου η απεικόνιση $\mathbb{Z} \xrightarrow{2} \mathbb{Z}$ είναι πολλαπλασιασμός με το 2, δεν διασπάται (γιατί;).

2) Έστω $k$ σώμα. Τότε κάθε ακριβής ακολουθία $k$ διανυσματικών χώρων πεπερασμένων διάστασης

$$0 \to V_1 \to V_2 \to V_3 \to 0$$

διασπάται, γιατί κάθε σύνολο γραμμικώς ανεξαρτήτων διανυσμάτων του $V_2$ μπορεί να επεκταθεί σε βάση του $V_2$.

3) Έστω $k$ ένα σώμα. Η ακριβής ακολουθία

$$0 \to (x) \to k[x] \to k \to 0$$

διασπάται, αν αυτή θεωρηθεί ως ακολουθία $k$-προτύπων: ορίζουμε $\alpha' : k[x] \mapsto (x)$, $\alpha'(f_0 + f_1 + ... + f_n x^n) = f_1 x + ... + f_n x^n$. Τότε ο $\alpha'$ είναι $k$ –ομομορφισμός και ο περιορισμός του στο $(x)$ είναι η ταυτοτική απεικόνιση. Όμως η παραπάνω ακριβής ακολουθία *δεν* διασπάται αν θεωρηθεί ως ακολουθία $k[x]$-προτύπων. Πράγματι, έστω $\alpha' : k[x] \mapsto (x)$ ομομορφισμός $k[x]$- προτύπων που είναι ταυτοτική στο $(x)$. Έστω $\alpha'(1) = xf(x)$, $f(x) \in k(x)$. Τότε $\alpha'(x) = x\alpha'(1) = x^2 f(x)$, δηλαδή $x = x^2 f(x)$. Φυσικά δεν υπάρχει τέτοιο $f(x)$.

## 3.4 Ελεύθερα Πρότυπα

Έστω $M$ ένα $R$-πρότυπο. Μια οικογένεια $(e_\lambda)_{\lambda \in \Lambda}$ στοιχείων του $M$ καλείται *βάση* του $M$ αν i) το σύνολο $\{e_\lambda \mid \lambda \in \Lambda\}$ παράγει το $M$, και ii) κάθε $m \in M$ γράφεται κατά μοναδικό τρόπο ως άθροισμα της μορφής $\sum_{\lambda \in \Lambda} r_\lambda e_\lambda$, όπου $r_\lambda \in R$ και όλα εκτός του πολύ ένα πεπερασμένο πλήθος από τα $r_\lambda$ είναι μηδέν.

*Ελεύθερο* λέγεται το πρότυπο που έχει μια τουλάχιστον βάση.
(Δεχόμαστε ότι το μηδενικό $R$-πρότυπο $(0)$ είναι ελεύθερο με μία βάση το κενό σύνολο.) Για παράδειγμα, το $R$ είναι ελεύθερο $R$-πρότυπο με βάση το μονοσύνολο $\{1\}$. Το $\mathbb{Z}$-πρότυπο $\mathbb{Z}\left[\sqrt{-2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$ είναι ελεύθερο με βάση $\{1, \sqrt{-2}\}$ (γιατί;).

**3.4.1 Πρόταση** *Ένα R-πρότυπο M είναι ελεύθερο αν και μόνο αν είναι ισόμορφο με ένα πρότυπο της μορφής* $\bigoplus_{\lambda\in\Lambda} R_\lambda$, *όπου* $R_\lambda = R$ *για κάθε* $\lambda \in \Lambda$.

**Απόδειξη.** Έστω ότι το $M$ είναι ελεύθερο με βάση $\{e_\lambda \mid \lambda \in \Lambda\}$. Κάθε στοιχείο $m \in M$ γράφεται κατά μοναδικό τρόπο στη μορφή $m = \sum_{\lambda\in\Lambda} r_\lambda e_\lambda$ όπου όλα τα $r_\lambda$ είναι μηδέν εκτός το πολύ ένα πεπερασμένο πλήθος. Άρα ορίζεται μια απεικόνιση

$$\varphi : M \ni m \mapsto (r_\lambda)_{\lambda\in\Lambda} \in \bigoplus_{\lambda\in\Lambda} R_\lambda$$

που είναι $R$-ισομορφισμός. Αντίστροφα, το $\bigoplus_{\lambda\in\Lambda} R_\lambda$ είναι ελεύθερο γιατί μία βάση του είναι το σύνολο $\{\varepsilon_\lambda \mid \lambda \in \Lambda\}$, όπου $\varepsilon_\lambda$ είναι η ακολουθία $\varepsilon_\lambda = (\varepsilon_\lambda)_\mu$ με $\varepsilon_{\lambda\mu} = 0$ αν $\lambda \neq \mu$ και $\varepsilon_{\lambda\mu} = 1$ αν $\lambda = \mu$. □

**3.4.2 Πόρισμα** *Κάθε R-πρότυπο M είναι ομομορφική εικόνα ελεύθερου R-πρότυπο.*

**Απόδειξη.** Έστω $\Lambda$ ένα σύνολο γεννητόρων $M$, για παράδειγμα $\Lambda = M$. Κατά τον προφανή τρόπο ορίζεται ένας $R$–επιμορφισμός $\bigoplus_{\lambda\in\Lambda} R_\lambda \to M$. □

Σε αντίθεση με την περίπτωση των διανυσματικών χώρων, υπάρχουν πολλά $R$-πρότυπα που δεν είναι ελεύθερα. Για παράδειγμα, το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_m (m > 1)$ δεν είναι ελεύθερο. Επίσης υποπρότυπο ελεύθερου προτύπου δεν είναι αναγκαστικά ελεύθερο. Ένα παράδειγμα υπάρχει στην Άσκηση 5. Ένα άλλο παράδειγμα είναι το $\mathbb{Z}_4$-πρότυπο $\{[0], [2]\} \subseteq \mathbb{Z}_4$. Θα δούμε όμως παρακάτω, ότι αν ο $R$ είναι περιοχή κυρίων ιδεωδών τότε κάθε υποπρότυπο ελεύθερου προτύπου πεπερασμένης τάξης είναι πάλι ελεύθερο. Αυτό θα βρει εφαρμογή στο Κεφάλαιο 9 όπου μελετάμε τους αλγεβρικούς ακέραιους ενός αριθμητικού σώματος.

Υπάρχουν λοιπόν πολλά μη ελεύθερα πρότυπα. Έτσι γεννιέται το ερώτημα: για ποιους δακτυλίου $R$ κάθε $R$-πρότυπο είναι ελεύθερο; Δες την Άσκηση 6.

**3.4.3 Πρόταση** *Έστω*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

*μια ακριβής ακολουθία $R$-προτύπων. Αν το $C$ είναι ελεύθερο, τότε η ακολουθία διασπάται.*

**Απόδειξη.** Έστω $\{e_\lambda\}_{\lambda\in\Lambda}$ μια βάση του $C$. Αφού ο $\beta$ είναι επιμορφισμός υπάρχουν $b_\lambda \in B, \lambda \in \Lambda$, με την ιδιότητα $\beta(b_\lambda) = e_\lambda$. Για αυτήν την επιλογή ορίζουμε έναν $R$-ομομορφισμό $\beta' : C \to B$ από τις σχέσεις

$$\beta'(e_\lambda) = b_\lambda .$$

(Για να ορίσουμε έναν $R$ – ομομορφισμό πάνω σ' ένα ελεύθερο $R$ – πρότυπο αρκεί να οριστεί η απεικόνιση πάνω σε μία βάση και να την επεκτείνουμε γραμμικά, όπως πράττουμε στους διανυσματικούς χώρους). Προφανώς $\beta \circ \beta' = 1_c$ και συνεπώς (Πρόταση 3.3.1) η ακολουθία διασπάται. □

Έχοντας αναπτύξει στις προηγούμενες παραγράφους τις πλέον στοιχειώδεις ιδιότητες προτύπων θα αποδείξουμε τώρα δύο σημαντικά αποτελέσματα. Το πρώτο λέει ότι οποιεσδήποτε δύο βάσεις ενός ελεύθερου $R$ – προτύπου, όπου $R$ μεταθετικός δακτύλιος με μονάδα, έχουν τον ίδιο πληθικό αριθμό. Αυτό δεν ισχύει γενικά για μη μεταθετικούς δακτυλίους (Σημείωση 3.6.2ii). Το δεύτερο αποτέλεσμα μας πληροφορεί ότι υποπρότυπο ελευθέρου προτύπου πάνω από περιοχή κυρίων ιδεωδών είναι ελεύθερο. Αυτό δεν ισχύει για γενικούς δακτυλίους. Πρώτα όμως χρειαζόμαστε το Λήμμα του Zorn.

## 3.5 Λήμμα του Zorn και Εφαρμογές

Έστω $X$ ένα μη κενό σύνολο. Μια σχέση $\leq$ στο $X$ ονομάζεται *σχέση μερικής διάταξης* αν i) $x \leq \forall x \in X$, ii) $x \leq y, y \leq z \Rightarrow x \leq z$, και iii) $x \leq y$, $y \leq x \Rightarrow x = y$. Είναι μη κενό σύνολο εφοδιασμένο με μία σχέση μερικής διάταξης καλείται *μερικά διατεταγμένο σύνολο*. Ένα μερικά διατεταγμένο σύνολο $X$ για το οποίο ισχύει η συνθήκη iv) για κάθε $x, y \in X$ είτε $y \leq x$, ονομάζεται ολικά *διατεταγμένο σύνολο*.

Έστω $Y$ ένα υποσύνολο του μερικά διατεταγμένου συνόλου $X$. Ένα στοιχείο $x \in X$ ονομάζεται *άνω φράγμα* του $Y$ αν $y \leq x$ για κάθε $y \in Y$.

Έστω στοιχείο $x \in X$ του μερικά διατεταγμένου συνόλου $X$ ονομάζεται *μέγιστο* αν $x \le x'$ με $x' \in X$ συνεπάγεται $x = x'$.

Μπορούμε τώρα να διατυπώσουμε το Λήμμα του Zorn. Στις σημειώσεις αυτές θα το εφαρμόσουμε αρκετές φορές ως ένα τυπικό εργαλείο σε αποδείξεις.

**3.5.1 Λήμμα του Zorn** *Έστω $X$ ένα μερικά διατεταγμένο σύνολο που έχει την ιδιότητα ότι κάθε μη κενό ολικά διατεταγμένο υποσύνολο του $X$ έχει ένα άνω φράγμα στο $X$. Τότε το $X$ έχει ένα τουλάχιστον μέγιστο στοιχείο.*

Αποδεικνύεται στη Θεωρία Συνόλων ότι το Λήμμα του Zorn είναι ισοδύναμο με το Αξίωμα Επιλογής. Βέβαια εμείς εδώ θα το δεχτούμε ως αξίωμα. Ακολουθεί μια πρώτη τυπική εφαρμογή.

**3.5.2 Πρόταση** *Έστω $R \neq 0$ ένας δακτύλιος. Τότε ο $R$ έχει ένα τουλάχιστον μέγιστο ιδεώδες.*

**Απόδειξη.** Έστω $X$ το σύνολο των γνήσιων ιδεωδών του $R$. Είναι $X \neq \varnothing$, αφού $R \neq \{0\}$. Ως σχέση μερικής διάταξης θεωρούμε τη σχέση $\subseteq$ υποσυνόλου. Έστω $Y$ ένα μη κενό ολικά διατεταγμένο υποσύνολο του $X$. Θέτουμε

$$J = \bigcup_{I \in Y} I .$$

Το $J$ είναι ιδεώδες του $R$. Πράγματι αν $a, b \in J$ τότε $a \in I_1$, και $b \in I_2$ για κάποια $I_1, I_2 \in Y$. Αλλά το $Y$ είναι ολικά διατεταγμένο. Συνεπώς $I_1 \subseteq I_2$ ή $I_2 \subseteq I_1$. Επομένως $a + b \in I_2$ ή $a + b \in I_1$, αντίστοιχα. Άρα $a + b \in J$. Επίσης, $ra \in I_1$ για κάθε $r \in R$ αφού το $I_1$ είναι ιδεώδες. Ισχύει $J \in X$ αφού το $J$ είναι γνήσιο ιδεώδες του $R$, γνήσιο γιατί αν $1 \in J$ τότε $1 \in I$ για κάποιο $I \in Y \subseteq X$ που δεν ισχύει. Άρα το $J$ είναι ένα άνω φράγμα του $Y$ στο $X$. Από το Λήμμα του Zorn συμπεραίνουμε ότι το $X$ έχει ένα μέγιστο στοιχείο $M$. Προφανώς το $M$ είναι μέγιστο ιδεώδες. □

Η παραπάνω απόδειξη είναι η αυστηρή διατύπωση της ιδέας: Έστω $I_1$ γνήσιο ιδεώδες του $R$. Αν δεν είναι μέγιστο, τότε περιέχεται γνήσια σε κάποιο άλλο $I_2$.

Αν το $I_2$ δεν είναι μέγιστο… Το Λήμμα του Zorn εγγυάται ότι η διαδικασία περατούται.

**3.5.3 Πόρισμα** *Κάθε γνήσιο ιδεώδες του R περιέχεται σ' ένα μέγιστο ιδεώδες.*

**Απόδειξη.** Έστω $I$ ένα γνήσιο ιδεώδες του $R$. Εφαρμόζουμε την Πρόταση 3.5.2 στο δακτύλιο $R/I$ οπότε υπάρχει μέγιστο ιδεώδες του $R/I$. Όμως αυτό έχει τη μορφή $M/I$ όπου $M$ μέγιστο ιδεώδες του $R$ που περιέχει το $I$ (Άσκηση 1.16). □

Η δεύτερη εφαρμογή του Λήμματος του Zorn αναφέρεται σε πρώτα ιδεώδη.

Ένα υποσύνολο $S \subseteq R$ ενός δακτυλίου $R$ λέγεται *πολλαπλασιαστικό*, αν i) $1 \in S$, και ii) $a,b \in S \Rightarrow ab \in S$.

Για παράδειγμα, αν $P$ είναι πρώτο ιδεώδες, το $R-P$ είναι πολλαπλασιαστικό σύνολο.

**3.5.4 Πρόταση** *Έστω R ένας δακτύλιος, $S \subseteq R$ ένα πολλαπλασιαστικό σύνολο, και $I$ ένα ιδεώδες του R με την ιδιότητα $I \cap S = \varnothing$. Τότε υπάρχει πρώτο ιδεώδες $P$ και $R$ με τις ιδιότητες $P \supseteq I$ και $P \cap S = \varnothing$.*

**Απόδειξη.** Έστω $X$ το σύνολο των ιδεωδών του $R$ που έχουν τις ιδιότητες $J \supseteq I$ και $J \cap S = \varnothing$. Είναι $X \neq \varnothing$, αφού $I \in X$. Ως σχέση μερικής διάταξης στο $X$ θεωρούμε τη σχέση $\subseteq$ υποσυνόλου. Έστω $Y$ ένα μη κενό ολικά διατεταγμένο υποσύνολο του $X$. Θέτουμε

$$J' = \bigcup_{J \in Y} I .$$

Όπως ακριβώς στην απόδειξη της Πρότασης 3.5.2 διαπιστώνουμε ότι ο $P$ είναι ιδεώδες. Προφανώς $J' \supseteq I$ και $J' \cap S = \varnothing$. Άρα $J' \in X$ και το $J'$ είναι ένα άνω φράγμα του $Y$ στο $X$. Συνεπώς από το Λήμμα του Zorn, το $X$ έχει ένα μέγιστο στοιχείο, έστω $P \in X$.

Θα δείξουμε ότι το $P$ είναι πρώτο ιδεώδες. Έστω $ab \in P$ με $a,b \in R$. Έστω ότι $a \in P$ και $b \in P$. Θα καταλήξουμε σε άτοπο. Τα ιδεώδη $P+(a)$ και $P+(b)$ περιέχουν το $I$ γιατί $I \subseteq P$. Επιπλέον $P \subsetneq P+(a)$ και $P \subsetneq P+(b)$. Άρα ο ορισμός του $P$ δίνει

$$P+(a)\cap S\neq\varnothing \text{ και } P+(b)\cap S\neq\varnothing .$$

Άρα $p+ra\in S$ και $q+sb\in S$ για κάποια $p,q\in P,\ r,s\in R$. Αφού το $S$ είναι πολλαπλασιαστικό παίρνουμε $(p+ra)(q+sb)\in S$, δηλαδή

$$(pq+psb+raq)+rasb\in S .$$

Αλλά το άθροισμα στην παρένθεση ανήκει στο $P$. Αφού $P\cap S=\varnothing$, έχουμε $rasb\notin P$. Άρα $ab\notin P$. □

Η χρησιμότητα της προηγούμενης πρότασης θα φανεί σε επόμενα κεφάλαια (π.χ. Πρόταση 6.1.2), ενώ η χρησιμότητα της Πρότασης 3.5.2 θα φανεί αμέσως παρακάτω.

## 3.6 Πληθάριθμος Βάσης Ελεύθερου Προτύπου

**3.6.1 Θεώρημα** *Έστω $R\neq\{0\}$ ένας δακτύλιος και $F$ ένα ελεύθερο $R$-πρότυπο που έχει μία πεπερασμένη βάση με $n$ στοιχεία. Τότε κάθε άλλη βάση του $F$ έχει $n$ στοιχεία.*

**Απόδειξη.** Έστω $\{e_1,...,e_n\}$ μια βάση του $F$ (μπορούμε να υποθέσουμε $n\neq 0$ δηλαδή $F\neq 0$). Αφού $R\neq\{0\}$, υπάρχει μέγιστο ιδεώδες $M$ του $R$ (Πρόταση 3.5.2). Σύμφωνα με την Άσκηση 12, το πρότυπο πηλίκο $F/MF$ είναι ένα $R/M$ - πρότυπο, δηλαδή είναι ένας $R/M$ - διανυσματικός χώρος (Πρόταση 0.6.4). Θα δείξουμε ότι τα στοιχεία $e_1+MF,...,e_n+MF$ αποτελούν μία βάση του $F/MF$.

Εφόσον το σύνολο $\{e_1,...,e_n\}$ παράγει το $F$ ως $R-$πρότυπο, είναι προφανές ότι τα στοιχεία $e_1+MF,...,e_n+MF$ παράγουν το $F/MF$ ως $R/M$ -πρότυπο.

Δείχνουμε τώρα ότι τα $e_1+MF,...,e_n+MF$ είναι γραμμικώς ανεξάρτητα στοιχεία του $F/MF$ πάνω από το $R/M$. Έστω

$$\sum_i (r_i+M)(e_i+MF)=MF,\ r_i\in R .$$

Τότε $\sum_i r_ie_i\in MF$. Γράφοντας

$$\sum_i r_ie_i=\sum_i a_ie_i,\ a_i\in M$$

συμπεραίνουμε ότι $r_i = a$ γιατί τα $e_i$, $i = 1,...n$, είναι βάση του $F$. Έτσι $r_i \in M$ και συνεπώς $r_i + M = M$ για κάθε $i = 1,...n$.

Αποδείξαμε λοιπόν ότι: $\{e_1,...,e_n\}$ βάση του $F \Rightarrow \{e_1 + M,...,e_n + M\}$ βάση του διανυσματικού χώρου $F/MF$. Επειδή τώρα κάθε δύο βάσεις ενός πεπερασμένα παραγόμενου διανυσματικού χώρου έχουν τον ίδιο πληθάριθμο (όπως θυμόμαστε από τη Γραμμική Άλγεβρα), προκύπτει το ζητούμενο. □

**3.6.2 Σημείωση** Το Θεώρημα 3.6.1 δεν ισχύει γενικά για μη μεταθετικούς δακτυλίους. Δίνουμε εδώ ένα κλασσικό παράδειγμα. Έστω $R$ ο δακτύλιος των ομομορφισμών αβελιανών ομάδων $\bigoplus_{i\in N} \mathbb{Z} \to \bigoplus_{i\in N} \mathbb{Z}$ όπου $\bigoplus_{i\in N} \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$ και $N = \{1,2,...\}$. Ο πολλαπλαπλασιασμός του $R$ είναι η σύνθεση συναρτήσεων. Θεωρώντας $R$ ως $R$- πρότυπο, είναι ελεύθερο (προφανώς) με βάση το μονοσύνολο $\{1_R\}$, όπου $1_R$ είναι η ταυτοτική απεικόνιση $\bigoplus_{i\in N} \mathbb{Z} \to \bigoplus_{i\in N} \mathbb{Z}$. Ορίζουμε τώρα μια άλλη βάση του $R$. Έστω

$$\{e_1, e_2,...\}$$

η κανονική βάση του $\bigoplus_{i\in N} \mathbb{Z}$ ως $\mathbb{Z}$-πρότυπο, δηλαδή $e_1 = (1,0,...)$, $e_2 = (0,1,0,...)$ κ.λ.π.. Έστω $f, g \in R$ που ορίζονται από τις σχέσεις

$$f(e_i) = \begin{cases} e_n, & \text{αν} \quad i = 2n \\ 0, & \text{αν} \quad i = 2n+1 \end{cases}$$

$$g(e_i) = \begin{cases} 0, & \text{αν} \quad i = 2n \\ e_n, & \text{αν} \quad i = 2n-1 \end{cases}$$

Τώρα κάθε στοιχείο $\varphi \in R$ γράφεται κατά μοναδικό τρόπο ως

$$\varphi \in \alpha f + \beta g, \quad \alpha, \beta \in R$$

(Μάλιστα $\alpha(e_i) = \varphi(e_{2i})$ και $\beta(e_i) = \varphi(e_{2i-1})$). Άρα μια άλλη βάση του $R$ είναι το $\{f, g\}$! Ο δακτύλιος $R$ σε ορισμένους αλγεβρικούς κύκλους είναι γνωστός ως ο "Μέγας Δακτύλιος" και είναι πηγή αρκετών αντιπαραδειγμάτων.

Το Θεώρημα 3.6.1 μας επιτρέπει να ορίσουμε την έννοια της τάξης ελεύθερου προτύπου.

**3.6.3 Ορισμός** *Έστω $F$ ένα ελεύθερο $R$-πρότυπο, όπου $R \neq \{0\}$. Ο πληθάριθμος μιας πεπερασμένης βάσης του $F$ ονομάζεται τάξη του $F$. Αν το $F$ δεν έχει πεπερασμένη βάση θα λέμε ότι η τάξη του είναι άπειρη. Η τάξη του $F$ συμβολίζεται $\operatorname{rank} F$.*

**3.6.4 Λήμμα** *Έστω $F_1, F_2$ ελεύθερα $R$-πρότυπα. Τότε το $F_1 \oplus F_2$ είναι ελεύθερο και $\operatorname{rank}(F_1 \oplus F_2) = \operatorname{rank} F_1 + \operatorname{rank} F_2$.*

**Απόδειξη.** Πρόταση 3.4.1 □

## 3.7 Υποπρότυπα Ελευθέρων Προτύπων

Δεν αληθεύει ότι κάθε υποπρότυπο ελεύθερου πρότυπου είναι ελεύθερο. Για παράδειγμα, έστω $R = \mathbb{Q}[x, y]$ και $I = (x, y)$. Το $I$ δεν είναι ελεύθερο $R$-πρότυπο (γιατί;). Η περίπτωση των περιοχών κυρίων ιδεωδών είναι πιο ευχάριστη:

**3.7.1 Θεώρημα** *Έστω $R$ περιοχή κυρίων ιδεωδών και $F$ ένα ελεύθερο $R$-πρότυπο με $\operatorname{rank} F = n < \infty$. Τότε κάθε υποπρότυπο $F' < F$ είναι ελεύθερο με $\operatorname{rank} F' \leq n$.*

**Απόδειξη.** Επαγωγή στο $n$. Για $n = 1$, έχουμε $F \cong R$, οπότε πρέπει να δείξουμε ότι κάθε ιδεώδες του $R$ είναι ελεύθερο $R$-πρότυπο. Κάθε ιδεώδες του $R$ έχει τη μορφή $I = (a)$ για κάποιο $a \in R$. Αν $a = 0$, τότε $I = (0)$ είναι ελεύθερο με τάξη 0. Αν $a \neq 0$, τότε ως $R$ - πρότυπα ισχύει $I \simeq R$, γιατί η απεικόνιση

$$R \ni r \mapsto ra \in I$$

είναι $R$-ισομορφισμός. Άρα σ' αυτήν την περίπτωση το $I$ είναι ελεύθερο με τάξη 1.

Υποθέτουμε τώρα $n > 1$ και ότι το θεώρημα ισχύει για όλα τα ελεύθερα $R$ - πρότυπα με τάξη $\leq n-1$. Έστω $\{e_1, ..., e_n\}$ βάση του $F$, οπότε $F = \langle e_1 \rangle + ... + \langle e_n \rangle$. Θέτουμε $\overline{F} = \langle e_2 \rangle + \cdots + \langle e_n \rangle$. Ισχύει $F' \cap \overline{F} \leq \overline{F}$ και το $\overline{F}$ έχει τάξη $n-1$. Άρα

το $F' \cap \overline{F}$ είναι ελεύθερο με τάξη $\leq n-1$. Ισχύει $F/\overline{F} \simeq \langle e_1 \rangle$ και άρα το $F/\overline{F}$ έχει τάξη 1.
Έστω

$$\varphi : F \to F/\overline{F}$$

ο φυσικός επιμορφισμός και

$$\varphi \mid F' : F' \to F/\overline{F}$$

ο περιορισμός του $\varphi$ στο $F'$. Επειδή το $F/\overline{F}$ είναι ελεύθερο τάξης 1, η εικόνα $\varphi(F')$ θα είναι ελεύθερο πρότυπο τάξης 0 ή 1. Έχουμε την ακριβή ακολουθία

$$0 \to \ker \varphi \mid F' \to F' \to \varphi(F') \to 0 .$$

Αυτή διασπάται (Πρόταση 3.4.3). Άρα $F' \simeq \ker \phi \mid F' \oplus \phi(F')$. Όμως $\ker \varphi \mid F' = \overline{F} \cap F'$ που από την επαγωγική υπόθεση είναι ελεύθερο με τάξη $\leq n-1$. Έτσι

$$F' \simeq (\overline{F} \cap F') \oplus \phi(F') .$$

Το δεξί μέλος είναι ευθύ άθροισμα ελεύθερων προτύπων και άρα ελεύθερο με $rank((\overline{F} \cap F') \oplus \varphi(F')) = rank(\overline{F} \cap F') + rank\varphi(F') \leq n-1+1 = n$ (Λήμμα 3.6.4).

□

## Ασκήσεις

**1.** Έστω $M$ ένα $R$-πρότυπο και $\varphi : M \to M$ ένας $R$-ομομορφισμός για τον οποίο ισχύει $\varphi^2 = \varphi$. Τότε $M = \ker \varphi \oplus \operatorname{Im} \varphi$.

**2.** Έστω $A, B$ υποπρότυπα του $R$-προτύπου $M$. Τότε υπάρχει ακριβής ακολουθία της μορφής

$$0 \to M/A \cap B \to M/A \times M/B \to M/(A+B) \to 0$$

**3.** Έστω $I$ και $J$ ιδεώδη του $R$. Τότε υπάρχει ακριβής ακολουθία της μορφής

$$0 \to I \cap J \to R \to R/I \times R/J \to R/(I+J) \to 0 .$$

**4.** Κάθε κυκλικό πρότυπο του $R$ είναι ισόμορφο με ένα πρότυπο της μορφής $R/I$ για κατάλληλο ιδεώδες $I$ του $R$.

**5.** Έστω $k$ ένα σώμα. Το ιδεώδες $(x, y)$ δεν είναι ελεύθερο ως $k[x, y]$-πρότυπο. Άρα δεν αληθεύει ότι κάθε υποπρότυπο ελεύθερου προτύπου είναι ελεύθερο.

**6.** Τα ακόλουθα είναι ισοδύναμα

(i) $R$ είναι σώμα.

(ii) Κάθε $R$-πρότυπο είναι ελεύθερο.

(iii) Κάθε κυκλικό $R$-πρότυπο είναι ελεύθερο.

(Υπόδειξη: για το (iii)$\Rightarrow$ (i) θεωρείστε $R/(a)$).

**7.** Διατυπώστε και αποδείξτε για πρότυπα μια πρόταση ανάλογη με την Πρόταση 0.3.3.

**8.** Έστω $0 \to A \to B \to C \to 0$ ακριβής ακολουθία $R$-προτύπων όπου τα $A$ και $C$ είναι πεπερασμένα παραγόμενα. Τότε και το $B$ είναι πεπερασμένα παραγόμενο.

**9.** Έστω $R$ περιοχή μοναδικής παραγοντοποίησης και $x, y \in R$ με μ.κ.δ. $(x, y) = 1$. Θεωρούμε το ιδεώδες $I = (x, y)$. Αποδείξτε ότι υπάρχει ακριβής ακολουθία $R$-προτύπων της μορφής

$$0 \to R \xrightarrow{\alpha} R \oplus R \xrightarrow{\beta} I \to 0$$

όπου $\alpha(r) = (ry, rx)$, και $\beta(r, s) = rx - sy$. Αυτή ονομάζεται *σύμπλοκο του Koszul* για το ζεύγος $(x, y)$.

**10.** Έστω $R$ ένας δακτύλιος. Τότε κάθε ιδεώδες του $R$ είναι ελεύθερο $R$-πρότυπο αν και μόνο αν ο $R$ είναι περιοχή κυρίων ιδεωδών.

**11.** Το $\mathbb{Q}$ είναι ελεύθερο $\mathbb{Z}$-πρότυπο; Έστω $R$ ακέραια περιοχή που δεν είναι σώμα. Το σώμα πηλίκων της $R$ είναι ελεύθερο $R$-πρότυπο;

**12.** Έστω $I$ ιδεώδες του $R$. Αν $M$ είναι ένα $R$-πρότυπο, ορίζουμε $IM$ ως το υποπρότυπο του $M$ που παράγεται από το σύνολο $\{am \mid a \in I, m \in M\}$. Τότε το $M / IM$ έχει τη δομή $R/I$-προτύπου, όπου

$$(r + I)(m + IM) = rm + IM$$

**13.** Αν κάθε πηλίκο οποιουδήποτε ελεύθερου $R$- πρότυπο είναι πάλι ελεύθερο, τότε ο $R$ είναι…

**14.** Είναι ο δακτύλιος $\mathbb{Z} \times \mathbb{Z}$ περιοχή κυρίων ιδεωδών; Είναι το ιδεώδες $\mathbb{Z} \times \{0\}$ ελεύθερο $\mathbb{Z} \times \mathbb{Z}$ πρότυπο;

**15.** Έστω $M, N$ υποπρότυπα ενός τρίτου $R$- προτύπου. Αν τα πρότυπα $M+N$ και $M \cap N$ είναι πεπραγμένα παραγόμενα, τότε και τα $M$ και $N$ είναι πεπερασμένα παραγόμενα.
(Υπόδειξη: Άσκηση 8).

**16.** Έστω

$$\cdots \to M_{i+1} \xrightarrow{\alpha_{i+1}} M_i \xrightarrow{\alpha_i} M_{i-1} \xrightarrow{\alpha_{i-1}} \cdots$$

ακριβής ακολουθία $R$-προτύπων. Έστω $N_i = \ker a_i = \operatorname{Im} a_{i+1}$.

Αποδείξτε ότι οι δύο ακολουθίες

$$\cdots \to M_{i+1} \to N_i \to 0,\ 0 \to N_i \to M_i \to M_{i-1} \to \cdots$$

είναι ακριβείς.

**17.** Έστω

$$0 \to F_n \to \cdots \to F_1 \to F_0 \to 0$$

ακριβής ακολουθία ελεύθερων $R$-προτύπων, όπου $R$ είναι περιοχή κυρίων ιδεωδών. Αν $rankF_i < \infty$ για κάθε $i = 1,..., n,$ αποδείξετε ότι

$$\sum_{i=0}^{n} (-1)^i rankF_i = 0$$

**18.** Αληθεύει ότι το $\mathbb{Z}$-πρότυπο $\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$, όπου $d \in N$, είναι ελεύθερο; Αν ναι, ποια είναι η τάξη του;

**19.** Αν $0 \to F \to M \to F' \to 0$ είναι ακριβής ακολουθία $R$-προτύπων και τα $F, F'$ είναι ελεύθερα, τότε και το $M$ είναι ελεύθερο.

# Κεφάλαιο 4

# Δακτύλιοι της Noether

Το 1890 ο Hilbert απέδειξε ότι κάθε ιδεώδες του πολυωνυμικού δακτυλίου $k[x_1,...,x_n]$, $k$ σώμα, είναι πεπερασμένα παραγόμενο. Η μέθοδός του δεν ήταν κατασκευαστική και προκάλεσε ισχυρή εντύπωση. Περίπου 30 χρόνια αργότερα η Emmy Noether αναγνώρισε ότι η συνθήκη αύξουσας αλυσίδας ιδεωδών ήταν η κρίσιμη ιδιότητα του $k[x_1,...,x_n]$ υπεύθυνη για το γεγονός ότι κάθε ιδεώδες του είναι πεπερασμένα παραγόμενο. Δακτύλιοι που ικανοποιούν αυτή τη συνθήκη ονομάζονται σήμερα δακτύλιοι της Noether. Αποτελούν κύριο αντικείμενο μελέτης της Μεταθετικής Άλγεβρας και Αλγεβρικής Γεωμετρίας και εμφανίζονται συχνότητα στην Αλγεβρική Θεωρία Αριθμών. Για παράδειγμα ο δακτύλιος των ακεραίων κάθε αριθμητικού σώματος είναι της Noether, πράγμα που θα αποδείξουμε στο Κεφάλαιο 9.

Στο Κεφάλαιο αυτό θα αποδείξουμε αρχικά το Θεώρημα Βάσης του Hilbert. Μετά θα αποδείξουμε ένα θεώρημα του I.S. Cohen, που λέει ότι αρκεί κάθε πρώτο ιδεώδες του $R$ να είναι πεπερασμένα παραγόμενο για να είναι κάθε ιδεώδες πεπερασμένα παραγόμενο. Ως εφαρμογή αυτού θα αποδείξουμε ένα θεώρημα για δυναμοσειρές ανάλογο με το Θεώρημα Βάσης του Hilbert.

## 4.1 Ορισμός και Παραδείγματα

**4.1.1 Πρόταση** *Έστω $R$ ένας δακτύλιος. Οι παρακάτω συνθήκες είναι ισοδύναμες.*

*(i) Κάθε αύξουσα ακολουθία ιδεωδών του $R$*

$$I_1 \subseteq I_2 \subseteq \cdots$$

*είναι τελικά σταθερή, δηλαδή υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε*

$$I_k = I_{k+1} = \cdots .$$

*(ii) Κάθε μη κενό σύνολο ιδεωδών του R έχει μέγιστο στοιχείο.*

*(iii) Κάθε ιδεώδες του R είναι πεπερασμένα παραγόμενο.*

**Απόδειξη.** (i) $\Rightarrow$ (ii). Έστω $\Omega$ ένα μη κενό σύνολο ιδεωδών του $R$ και $I_1 \in \Omega$. Αν το $I_1$ δεν είναι μέγιστο στοιχείο του $\Omega$, τότε υπάρχει $I_2 \in \Omega$ με

$$I_1 \subsetneq I_2 .$$

Αν το $I_2$ δεν είναι μέγιστο στοιχείο του $\Omega$, τότε … κ.λ.π. Λόγω της (i), η διαδικασία αυτή περατούται μετά από ένα πεπερασμένο πλήθος βημάτων, έστω $k$. Προφανώς το $I_k$ είναι μέγιστο στοιχείο του $\Omega$.

(ii) $\Rightarrow$ (iii). Έστω $I$ ιδεώδες του $R$ και έστω $\Omega$ το σύνολο των πεπερασμένων παραγόμενων ιδεωδών του $R$ που περιέχονται στο $I$. Τότε $\Omega \neq \varnothing$ αφού $(0) \in \Omega$. Έστω $J$ ένα μέγιστο στοιχείο του $\Omega$. Αν $J \neq I$ τότε υπάρχει $a \in I - J$. Το ιδεώδες $J + (a)$ περιέχεται προφανώς στο $\Omega$. Άρα $J = I$ και το $I$ είναι πεπερασμένα παραγόμενο.

(iii) $\Rightarrow$ (i). Έστω

$$I_1 \subseteq I_2 \subseteq \cdots$$

μια ακολουθία ιδεωδών του $R$. Θέτουμε $J = \bigcup_i I_i$. Εύκολα ελέγχουμε ότι το $J$ είναι ιδεώδες (δες και την απόδειξη της Πρότασης 3.5.2). Άρα το $J$ είναι πεπερασμένα παραγόμενο. Έστω $J = (a_1, ..., a_m)$. Έχουμε $a_i \in I_{n_i}$ για κάποια $n_i$. Αν $n = \max\{n_i \mid i = 1, ..., m\}$, τότε $a_i \in I_n$ για κάθε $i = 1, ..., m$. Άρα $J \subseteq I_n$. Τότε βέβαια για την ακολουθία ισχύει

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n = I_{n+1} = \cdots . \qquad \square$$

**4.1.2 Ορισμός** *Ένας δακτύλιος που ικανοποιεί μια από τις συνθήκες της Πρότασης 4.1.1 ονομάζεται δακτύλιος της Noether.*

**4.1.3 Παράδειγμα** 1) Κάθε περιοχή κυρίων ιδεωδών είναι δακτύλιος της Noether. Άρα ο $\mathbb{Z}$ και ο $k[x]$, $k$ σώμα, είναι δακτύλιος της Noether.

2) Κάθε πεπερασμένος δακτύλιος είναι της Noether.

3) Ο δακτύλιος $k[x_1, x_2, ...]$ των πολυωνύμων στις (απείρου πλήθους) μεταβλητές $x_1, x_2, ...$ δεν είναι της Noether αφού $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$.

**4.1.4 Πρόταση** *Έστω $\varphi : R \to S$ ένας επιμορφισμός δακτυλίων. Αν ο R είναι της Noether, τότε και ο S είναι της Noether.*

**Απόδειξη.** Έστω $I = \ker \varphi$. Αρκεί (Θεώρημα 0.3.2) να δείξουμε ότι ο $R/I$ είναι της Noether. Έστω

$$J_1 \subseteq J_2 \subseteq \cdots$$

μια ακολουθία ιδεωδών του $R/I$. Από την Πρόταση 0.3.3, κάθε $J_i$ έχει τη μορφή $I_i / I$ για κάποιο ιδεώδες $I_i \supseteq I$ του *R*. Συνεπώς

$$I_1 \subseteq I_2 \subseteq \cdots.$$

Αφού ο $R$ είναι της Noether, έχουμε $I_m = I_{m+1} = \cdots$ για κάποιο *m*. Άρα $J_m = J_{m+1} = \cdots$. □

## 4.2 Θεώρημα Βάσης του Hilbert

**4.2.1 Θεώρημα** *(Θεώρημα Βάσης του Hilbert). Έστω R ένας δακτύλιος της Noether. Τότε και ο $R[x]$ είναι δακτύλιος της Noether.*

**Απόδειξη.** Έστω *I* ιδεώδες του $R[x]$. Θα δείξουμε ότι το *I* είναι πεπερασμένα παραγόμενο. Ορίζουμε

$$J_n = \{r \in R \mid \text{υπάρχει } rx^n + t_{n-1}x^{n-1} + \cdots + r_0 \in I\}$$

Δηλαδή το $J_n$ περιέχει το 0 και τους μεγιστοβάθμιους συντελεστές των πολυωνύμων βαθμού *n* που περιέχονται στο *I*. Χρησιμοποιώντας το γεγονός ότι το *I* είναι ιδεώδες, εύκολα δείχνουμε ότι το $J_n$ είναι ιδεώδες. Επίσης ισχύει $J_n \subseteq J_{n+1}$, γιατί $f \in I \Rightarrow xf \in I$. Έτσι έχουμε μια αύξουσα ακολουθία ιδεωδών του *R*.

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots.$$

Εφόσον ο *R* είναι της Noether, έχουμε

$$J_N = J_{N+1} = \cdots$$

για κάποιο $N \in \mathbb{N}$.

Για κάθε $i = 0,1,...,N$ έστω $r_{i1}, r_{i2}, ..., r_{im_i}$ γεννήτορες του $J_i$ (ο $R$ είναι της Noether). Έστω αντίστοιχα πολυώνυμα

$$f_{ik} = r_{ik} x^i + \cdots \in I \tag{1}$$

με βαθμό $i$ και μεγιστοβάθμιο συντελεστή $r_{ik}$, όπου $i = 0,1,...,N$ και $k = 1,2,...,m_i$. Θα δείξουμε τώρα ότι τα πολυώνυμα στην (1) παράγουν το $I$. Έστω $f \in I$. Αν $sx^n$ είναι ο μεγιστοβάθμιος όρος του $f$ τότε $s \in J_n$ από τον ορισμό.

$1^{\eta}$ περίπτωση: $n \le N$. Τότε γράφουμε

$$s = \sum_j b_j r_{n,j}$$

για κάποια $b_j \in R$, οπότε το πολυώνυμο

$$f - \sum_j b_j f_{n,j} \tag{2}$$

έχει βαθμό $< n$.

$2^{\eta}$ περίπτωση: $n > N$. Τότε $s \in J_n = J_N$ και γράφουμε

$$s = \sum_j b_j r_{N,j}$$

για κάποια $b_j \in R$, οπότε το πολυώνυμο

$$f - x^{n-N} \sum b_j f_{N,j} \tag{3}$$

έχει βαθμό $< n$.

Τώρα από τις σχέσεις (2) και (3) προκύπτει άμεσα με επαγωγή στο $n(= \deg f)$ ότι το $f$ γράφεται ως γραμμικός συνδυασμός των $f_{ik}$ $(i = 0,...,N, k = 1,...,m_i)$. □

**4.2.2 Πόρισμα** *Έστω R ένας δακτύλιος της Noether. Τότε*

*(i) Ο* $R[x_1,...,x_n]$ *είναι δακτύλιος της Nother. Ειδικά οι* $\mathbb{Z}[x_1,...,x_n]$ *και* $k[x_1,...,x_n]$ *(k σώμα) είναι δακτύλιοι της Noether.*

*(ii) Κάθε πεπερασμένα παραγόμενη k-άλγεβρα είναι δακτύλιος της Noether.*

**Απόδειξη.** i) Με άμεση επαγωγή στο $n$ δείχνεται ότι ο $R[x_1,...,x_n]$ είναι της Noether.

ii) Κάθε πεπερασμένα παραγόμενη $k$-άλγεβρα είναι ομομορφική εικόνα του $k[x_1,...,x_n]$. Από το i), ο $k[x_1,...,x_n]$ είναι της Noether. Από την Πρόταση 4.1.4, κάθε ομομορφική εικόνα του $k[x_1,...,x_n]$ είναι της Noether. □

Τα προηγούμενα αποτελέσματα παρέχουν πληθώρα παραδειγμάτων δακτυλίων της Noether. Στο παρακάτω παράδειγμα θα δούμε ότι υποδακτύλιος ενός δακτυλίου της Noether *δεν* είναι αναγκαστικά της Noether.

**4.2.3 Παράδειγμα** Έστω $R = \mathbb{Z}[x, y]$, που είναι δακτύλιος της Noether. Έστω ο υποδακτύλιος $S \subseteq R$

$$S = \{a + xf(x, y) \mid a \in \mathbb{Z} \quad \text{και} \quad f(x, y) \in \mathbb{Z}[x, y]\}.$$

Μια γνήσια αύξουσα ακολουθιών ιδεωδών του $S$ είναι

$$(x) \underset{\neq}{\subseteq} (x, xy) \underset{\neq}{\subseteq} (x, xy, xy^2) \underset{\neq}{\subseteq} \cdots$$

(γιατί;). Άρα ο $S$ είναι της Noether.

## 4.3 Πρώτα Ιδεώδη και Δυναμοσειρές

**4.3.1 Θεώρημα** *Αν κάθε πρώτο ιδεώδες του $R$ είναι πεπερασμένα παραγόμενο, τότε ο $R$ είναι δακτύλιος της Noether.*

**Απόδειξη.** Έστω ότι ο $R$ δεν είναι δακτύλιος της Noether. Θα αποδείξουμε ότι υπάρχει πρώτο ιδεώδες που δεν είναι πεπερασμένα παραγόμενο.

Έστω

$$\Omega = \{I \mid I \text{ ιδεώδες του } R \text{ που δεν είναι πεπερασμένα παραγόμενο}\}.$$

Τότε $\Omega \neq \varnothing$, γιατί ο $R$ δεν είναι της Noether. Θεωρούμε στο $\Omega$ τη σχέση μερικής διάταξης που δίνεται από τη σχέση υποσυνόλου $\subseteq$. Έστω $Y$ ένα μη κενό υποσύνολο του $\Omega$ που είναι ολικά διατεταγμένο. Θέτουμε

$$J = \bigcup_{I \in Y} I.$$

Εύκολα δείχνουμε ότι το $J$ είναι ιδεώδες (όπως στην απόδειξη της Πρότασης 4.1.1.). Θα δείξουμε ότι $J$ είναι ένα άνω φράγμα του $Y$ στο $\Omega$. Αρκεί να δείξουμε ότι $J \in \Omega$, δηλαδή ότι το $J$ δεν είναι πεπερασμένα παραγόμενο.

Έστω (για άτοπο) ότι το $J$ είναι πεπερασμένα παραγόμενο, $J = (a_1,...,a_t)$. Κάθε $a_i$ ανήκει σε κάποιο $I_i \in Y$ γιατί $J = \bigcup_{I \in Y} I$. Επειδή το $Y$ είναι ολικά διατεταγμένο, συμπεραίνουμε ότι για κάποιο $N \in \mathbb{N}$ ισχύει $a_1,...,a_t \in I_N$. Άρα $J \subseteq I_N$ και συνεπώς $J = I_N$. Δηλαδή $J = I_N = (a_1,...,a_t)$ που είναι πεπερασμένα παραγόμενο, άτοπο. Άρα $J \in \Omega$.

Εφαρμόζουμε τώρα το Λήμμα του Zorn (3.5.1): Το $\Omega$ έχει μέγιστο στοιχείο, έστω $P$. Θα δείξουμε ότι το $P$ είναι πρώτο. Επειδή δεν είναι πεπερασμένα παραγόμενο, θα έχουμε φτάσει στο επιθυμητό άτοπο.

Έστω $a,b \in R - P$ (ισχύει βέβαια $P \neq R$ γιατί το $R$ είναι πεπερασμένα παραγόμενο) και $ab \in P$. Θα φθάσουμε σε άτοπο. Επειδή $P \subsetneq P + (a)$, έχουμε ότι το $P + (a)$ είναι πεπερασμένα παραγόμενο λόγω του ορισμού του $P$. Άρα

$$P + (a) = (p_1 + r_1 a_1,..., p_n + r_n a)$$

για κάποια $p_i \in P$ και $r_i \in R$. Έστω $K = (P : (a)) = \{r \in R \mid ra \in P\}$ (§ 0.4). Επειδή $K \supseteq P + (b) \supsetneq P$, έχουμε ότι το $K$ είναι πεπερασμένα παραγόμενο. Συνεπώς και το ιδεώδες $aK$ είναι πεπερασμένα παραγόμενο.

Ισχυριζόμαστε ότι $P = (p_1,..., p_n) + aK$, που είναι βέβαια άτοπο. Η σχέση $P \supseteq (p_1,..., p_n) + aK$ είναι προφανής. Έστω $r \in P$. Τότε $r \in P + (a)$ και άρα

$$r = c_1(p_1 + r_1 a) + \cdots + c_n(p_n + r_n a)$$

για κάποια $c_i \in R$. Η παραπάνω σχέση γράφεται

$$(c_1 r_1 + \cdots + c_n r_n)a = r - (c_1 p_1 + \cdots + c_n p_n) \in P .$$

Άρα $c_1 r_1 + \cdots + c_n r_n \in K$. Τέλος

$$r = (c_1 p_1 + \cdots + c_n p_n) + (c_1 r_1 + \cdots + c_n r_n)a \in (p_1,..., p_n) + aK .$$

Αποδείξαμε έτσι τον ισχυρισμό και κατά συνέπεια το Θεώρημα. □

Εφαρμόζοντας το προηγούμενο θεώρημα θα αποδείξουμε τώρα ένα θεώρημα για δυναμοσειρές (§ 0.1) ανάλογο με το Θεώρημα Βάσης του Hilbert.

**4.3.2. Θεώρημα** *αν $R$ είναι δακτύλιος της Noether, τότε και ο $R[[x]]$ είναι δακτύλιος της Noether.*

**Απόδειξη.** Έστω $P$ ένα πρώτο ιδεώδες του $R[[x]]$. Θα δείξουμε ότι είναι πεπερασμένο παραγόμενο (4.3.1 Θεώρημα).

Η απεικόνιση

$$\varphi : R[[x]] \to R, \qquad r_0 + r_1 x + \cdots \mapsto r_0$$

είναι επιμορφισμός δακτυλίων. Άρα το $\varphi(P)$ είναι ιδεώδες του $R$ (Άσκηση 0.14). Από την υπόθεση το $\varphi(P)$ είναι πεπερασμένα παραγόμενο

$$\varphi(P) = (a_0^{(i)}, ..., a_0^{(t)}) .$$

Θεωρούμε αντίστοιχες δυναμοσειρές

$$f^{(i)} = a_0^{(i)} x + \cdots \in P .$$

*1η περίπτωση:* Έστω $x \in P$. Τότε γράφοντας

$$a_0^{(i)} = f^{(i)} - x(a_1^{(i)} + a_2^{(i)} x + \cdots)$$

βλέπουμε ότι $a_0^{(i)} \in P$ για κάθε $i = 1, ..., t$. Ισχυριζόμαστε ότι

$$P = (x, a_0^{(1)}, a_0^{(2)}, ..., a_0^{(t)}) .$$

Έστω $b_0 + b_1 x + \cdots \in P$. Τότε

$$b_0 = \varphi(b_0 + b_1 x + \cdots) \in \varphi(P) = (a_0^{(1)}, ..., a_0^{(t)}) ,$$

οπότε

$$b_0 + b_1 x + \cdots = b_0 + x(b_1 + b_2 x + \cdots +) \in (x, a_0^{(1)}, a_0^{(2)}, ..., a_0^{(t)}) .$$

*2η περίπτωση:* Έστω $x \notin P$. Θα δείξουμε ότι

$$P = (f^{(1)}, f^{(2)}, ..., f^{(t)}) .$$

Έστω $f = b_0 + b_1 x + \cdots \in P$.

*Ισχυρισμός:* Για κάθε $m \in \mathbb{N}$ υπάρχουν στοιχεία

$$b_0^{(1)}, ..., b_0^{(t)}, b_1^{(1)}, ..., b_1^{(t)}, ..., b_m^{(1)}, ..., b_m^{(t)} \in R$$

με την ιδιότητα

$$f - \sum_{i=1}^{t} \left( \sum_{j=0}^{m-1} b_j^{(i)} x^j \right) f^{(i)} = x^m g_m , \qquad g_m \in R[[x]] . \tag{4}$$

Ας δεχτούμε προς στιγμή τον ισχυρισμό για να δούμε πως ολοκληρώνεται η απόδειξη. Θέτοντας

$$e^{(i)} = b_0^{(i)} + b_1^{(i)}x + \cdots \in R[[x]]$$

έχουμε

$$f - \sum_{i=1}^{t} e^{(i)} f^{(i)} = x^m g_m - \sum_{i=1}^{t} \left( \sum_{j=m}^{\infty} b_j^{(i)} x^j \right) f^{(i)} \in (x^m),$$

για κάθε $m \in \mathbb{N}$. Αλλά στο $R[[x]]$ ισχύει προφανώς $\bigcap_{m\in\mathbb{N}} (x^m) = 0$. Άρα

$$f = \sum_{i=1}^{t} e^{(i)} f^{(i)} \in P.$$

*Απόδειξη του Ισχυρισμού:* Επαγωγή στο *m*. Για $m = 1$ παρατηρούμε ότι

$$b_0 = \varphi(b_0 + b_1 x + \cdots) \in \varphi(P) = (a_0^{(i)}, ..., a_0^{(t)}).$$

Έτσι

$$b_0 = b_0^{(1)} a_0^{(1)} + \cdots + b_0^{(t)} a_0^{(t)}, \quad b_0^{(i)} \in R.$$

Ισχύει επομένως

$$f - (b_0^{(1)} a_0^{(1)} + \cdots + b_0^{(t)} a_0^{(t)}) = x g_1, \quad g_1 \in R[[x]]$$

γιατί ο σταθερός όρος του αριστερού σκέλους είναι μηδέν. Υποθέτουμε ότι ισχύει ο ισχυρισμός για *m*. Τότε το αριστερό σκέλος της (4) ανήκει στο *P*. Άρα $x^m g_m \in P$. Επειδή $x \notin P$ και το *P* είναι πρώτο, παίρνουμε $g_m \in P$. Όπως στην περίπτωση $m = 1$, έχουμε για το $g_m \in P$ ότι υπάρχουν $b_m^{(1)}, ..., b_m^{(t)} \in R$ και $g_{m+1} \in R[[x]]$ με την ιδιότητα

$$g_m - (b_m^{(1)} f^{(1)} + \cdots + b_m^{(t)} f^{(t)}) = x g_{m+1}.$$

Τέλος από την επαγωγική υπόθεση και την προηγούμενη σχέση έχουμε:

$$\begin{aligned} f - \sum_{i=1}^{t} \left( \sum_{j=0}^{m-1} b_j^{(i)} x^j \right) f^{(i)} &= f - \sum_{i=1}^{t} \left( \sum_{j=0}^{m-1} b_j^{(i)} x^i \right) f^{(i)} - \sum_{i=1}^{t} (b_m^{(i)} x^m) f^{(i)} \\ &= x^m g_m - x^m (g_m - x g_{m+1}) \\ &= x^{m+1} g_{m+1}. \end{aligned}$$

□

**Σημείωση:** Είναι δυνατόν να αποδειχθεί το Θεώρημα 4.3.2 με τρόπο ανάλογο με την απόδειξη του Θεωρήματος Βάσης του Hilbert.

## Ασκήσεις

**1.** Ισχύει το αντίστροφο του Θεωρήματος Βάσης του Hilbert; Το αντίστροφο του Θεωρήματος 4.3.2;

**2.** Έστω $R$ ένας δακτύλιος της Noether και $\varphi : R \to R$ ένας επιμορφισμός δακτυλίων. Τότε ο $\varphi$ είναι ισομορφισμός (Υπόδειξη: $\ker\varphi \subseteq \ker\varphi^2 \subseteq \ker\varphi^3 \subseteq \cdots$).

**3*.** Ένα γνήσιο ιδεώδες $I$ του $R$ λέγεται *ανάγωγο* αν $I = I_1 \cap I_2 \Rightarrow I = I_1$ ή $I = I_2$ (όπου $(I_1, I_2$ είναι ιδεώδη του $R$). Έστω $R$ δακτύλιος της Noether. Τότε κάθε γνήσιο ιδεώδες του $R$ είναι τομή πεπερασμένου πλήθους ανάγωγων ιδεωδών. (Υπόδειξη: Έστω $\Omega$ το σύνολο των γνήσιων ιδεωδών του $R$ που δεν είναι τομές πεπερασμένου πλήθους του $R$. Δείξτε ότι $\Omega = \varnothing$ ).

**4.** Αποδείξτε ότι ο $\mathbb{Z}[x]$ είναι δακτύλιος της Noether χωρίς να χρησιμοποιήσετε το Θεώρημα Βάσης του Hilbert (Υπόδειξη: Θεώρημα 4.3.1).

**5.** Έστω $R$ ένας δακτύλιος της Noether. Τότε υπάρχει μονομορφισμός $R$-προτύπων της μορφής $R/P \to R$ για κάποιο πρώτο ιδεώδες $P$.

**6.** Δυο συστήματα πολυωνυμικών εξισώσεων λέγονται ισοδύναμα αν τα σύνολα των λύσεών τους ταυτίζονται. Αποδείξτε ότι κάθε άπειρο σύστημα $f_1 = f_2 = \cdots = 0$ ( $f_i \in k[x_1,...,x_n]$, $k$ σώμα) είναι ισοδύναμο με ένα πεπερασμένο σύστημα $f_{i_1} = f_{i_2} = \cdots = f_{i_m} = 0$.

Οι επόμενες δύο ασκήσεις δεν αφορούν δακτυλίους της Noether. Όμως δείχνουν πόσο ισχυρή είναι η τεχνική της απόδειξης του Θεωρήματος 4.3.1.

**7.** Κάθε γνήσιο ιδεώδες $P$ του $R$ μέγιστο (ως προς τη σχέση υποσυνόλου) ανάμεσα στα μη κύρια ιδεώδη του $R$ είναι πρώτο. (Υπόδειξη: Έστω $ab \in P$, $a \notin P$, $b \notin P$. Θεωρείστε $P \subsetneq P + (a) = (a')$ και $P \subsetneq \{r \mid ra' \in P\} = (a'')$. Δείξτε ότι $P = (a'a'')$, άτοπο).

**8.** Αν κάθε πρώτο ιδεώδες του $R$ είναι κύριο, τότε κάθε ιδεώδες του $R$ είναι κύριο. (Υπόδειξη: Έστω ότι το σύνολο των μη κύριων ιδεωδών είναι μη κενό.

Εφαρμόστε το Λήμμα του Zorn. Κάθε μέγιστο στοιχείο θα είναι κύριο από την προηγούμενη άσκηση, πράγμα άτοπο!).

# Κεφάλαιο 5

# Συνθήκες Αλυσίδων και Πρότυπα

Στο κεφάλαιο αυτό θα μελετήσουμε τη συνθήκη της αύξουσας αλυσίδας προτύπων (πρότυπα της Noether) και τη συνθήκη της φθίνουσας αλυσίδας προτύπων (πρότυπα του Artin). Οι αποδείξεις έχουν τυπικό χαρακτήρα και τα αποτελέσματα παρουσιάζουν κάποια συμμετρία. Αυτή όμως θα πάψει να υπάρχει όταν ασχοληθούμε στο Κεφάλαιο 6 με δακτυλίους του Artin, όπου θα έχουμε την ευκαιρία να εφαρμόσουμε τα αποτελέσματα του παρόντος κεφαλαίου.

## 5.1 Ορισμοί και Παραδείγματα

**5.1.1 Πρόταση** *Έστω $M$ ένα $R$-πρότυπο. Τότε οι παρακάτω συνθήκες είναι ισοδύναμες.*

*(i) Κάθε αύξουσα ακολουθία υποπροτύπων του $M$*

$$M_1 \subseteq M_2 \subseteq \cdots$$

*είναι τελικά σταθερή, δηλαδή υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε*

$$M_k = M_{k+1} = \cdots.$$

*(ii) Κάθε μη κενό σύνολο υποπρποτύπων του $M$ έχει μέγιστο στοιχείο.*

*(iii) Κάθε υποπρότυπο του $M$ είναι πεπερασμένα παραγόμενο.*

**Απόδειξη.** Δες την απόδειξη της Πρότασης 4.1.1. □

**5.1.2 Πρόταση** *Έστω $M$ ένα $R$-πρότυπο. Τότε οι παρακάτω συνθήκες είναι ισοδύναμες.*

*(i) Κάθε φθίνουσα ακολουθία υποπροτύπων του $M$*

$$M_1 \supseteq M_2 \supseteq \cdots$$

*είναι τελικά σταθερή, δηλαδή υπάρχει* $k \in \mathbb{N}$ *τέτοιο ώστε*

$$M_k = M_{k+1} = \cdots.$$

*(iii) Κάθε μη κενό σύνολο υποπροτύπων του M έχει ελάχιστο στοιχείο.*

**Απόδειξη.** Άσκηση. □

**5.1.3 Ορισμός** *Έστω M ένα R-πρότυπο.*

*(i) Το M ονομάζεται πρότυπο της Noether αν ικανοποιεί μια από τις συνθήκες της Πρότασης 5.1.1.*

*(ii) Το M ονομάζεται πρότυπο του Artin αν ικανοποιεί μια από τις συνθήκες της Πρότασης 5.1.2.*

Για παράδειγμα, ένας δακτύλιος *R* είναι *R*-πρότυπο της Noether αν και μόνον αν είναι δακτύλιος της Noether (Ορισμός 4.1.2). Λογικό είναι να ορίσουμε την έννοια του δακτυλίου του Artin κατ' ανάλογο τρόπο.

**5.1.4 Ορισμός** *Ένας δακτύλιος R ονομάζεται δακτύλιος του Artin αν είναι R-πρότυπο του Artin.*

Επομένως ο δακτύλιος *R* είναι του Artin ακριβώς όταν κάθε φθίνουσα αλυσίδα ιδεωδών του *R* είναι τελικά σταθερή.

**5.1.5 Παράδειγμα** 1) Ο $\mathbb{Z}$ είναι δακτύλιος της Noether όπως γνωρίζουμε, αλλά όχι του Artin, γιατί

$$(2) \supsetneq (2^2) \supsetneq (2^3) \supsetneq \cdots.$$

(2) Κάθε σώμα είναι δακτύλιος και της Noether και του Artin.

(3) Ο δακτύλιος $k[x_1, x_2, ...]$ δεν είναι ούτε της Noether ούτε του Artin, γιατί

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$$

και

$$(x_1) \supsetneq (x_1^2) \supsetneq (x_1^3) \supsetneq \cdots.$$

Θα δούμε στο επόμενο κεφάλαιο ότι κάθε δακτύλιος του Artin είναι δακτύλιος της Noether. Όμως για πρότυπα αυτό δεν ισχύει όπως δείχνει το παρακάτω κλασσικό παράδειγμα.

**5.1.6 Παράδειγμα** Έστω $p \in \mathbb{Z}$ ένας πρώτος αριθμός και $M$ το παρακάτω $\mathbb{Z}$-υποπρότυπο του $\mathbb{Q}/\mathbb{Z}$

$$M = \left\{ a \in \mathbb{Q}/\mathbb{Z} \mid a = \frac{r}{p^n} + \mathbb{Z},\ r \in \mathbb{Z},\ n \in \mathbb{N} \right\}.$$

Θέτουμε για κάθε $t \in \mathbb{N}$,

$$N_t = \left\{ a \in \mathbb{Q}/\mathbb{Z} \mid a = \frac{r}{p^t} + \mathbb{Z},\ r \in \mathbb{Z} \right\}.$$

Τότε ισχύουν

(i) Ως υποπρότυπα του $M$ έχουμε $N_t = \left\langle \frac{1}{p^t} + \mathbb{Z} \right\rangle$

(ii) Κάθε γνήσιο υποπρότυπο του $M$ έχει τη μορφή $N_t$ για κάποιο $t$

(iii) Ισχύει

$$N_0 \subsetneq N_1 \subsetneq \cdots$$

(iv) Το $N$ είναι $\mathbb{Z}$-πρότυπο του Artin αλλά όχι $\mathbb{Z}$-πρότυπο της Noether.

**Απόδειξη.** (i) Προφανές αφού $\frac{r}{p^t} + \mathbb{Z} = r\left( \frac{1}{p^t} + \mathbb{Z} \right)$.

(ii) Έστω $H \leq M$ με $H \neq 0$. Τότε υπάρχει $a \in H$ και γράφουμε $a = \frac{r}{p^t} + \mathbb{Z}$.

Μπορούμε να υποθέσουμε ότι $p$ δεν διαιρεί το $r$. Έστω τώρα

$$\frac{r_1}{p^{t_1}} + \mathbb{Z} \in H,\ p \text{ δεν διαιρεί το } r_1.$$

Θα δείξουμε ότι $\frac{1}{p^{t_1}} + \mathbb{Z} \in H$. Αφού μ.κ.δ.$(p, r_1) = 1$ τότε υπάρχουν (Άσκηση 1.13) $x, y \in \mathbb{Z}$ με

$$xr_1 + yp^{t_1} = 1.$$

Έχουμε τότε

$$\frac{1}{p^{t_1}} + \mathbb{Z} = \frac{xr_1 + yp^{t_1}}{p^{t_1}} + \mathbb{Z} = \frac{xr_1}{p^{t_1}} + \mathbb{Z} \in H .$$

Συνεπώς $N_t \subseteq H$ από το (i). Θα δείξουμε τώρα $H = N_m$ για κάποιο $m$. Παρατηρούμε ότι

$$M = \bigcup_{t \in \mathbb{N}} N_t$$

και

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots .$$

Επειδή το $H$ είναι γνήσιο υποπρότυπο του $M$ υπάρχει μέγιστο $m$ τέτοιο ώστε $N_m \subseteq H$ (γιατί;). Θα δείξουμε τώρα ότι $H = N_m$. Έστω (για άτοπο)

$$b = \frac{r_2}{p^{t_2}} + \mathbb{Z} \in H - N_m , \quad \text{μ.κ.δ.}(p, r_2) = 1 .$$

Αφού $b \notin N_m$ έχουμε $t_2 > m$. Αλλά όπως πριν συμπεραίνουμε $N_{t_2} \subseteq H$, άτοπο.

(iii) Αν $N_i = N_{i+1}$, τότε $\frac{1}{p^{i+1}} + \mathbb{Z} = \frac{r}{p^i} + \mathbb{Z}$ για κάποιο $r \in \mathbb{Z}$. Τότε

$$\frac{1}{p^{i+1}} - \frac{r}{p^i} \in \mathbb{Z}$$

δηλαδή $1 - rp = cp^{i+1}$ για κάποιο $I$, που είναι βέβαια άτοπο.

(iv) Κάθε φθίνουσα αλυσίδα υποπροτύπων του $M$ έχει τη μορφή

$$N_{t_1} \supseteq N_{t_2} \supseteq N_{t_3} \supseteq \cdots, \quad t_1 \geq t_2 \geq t_3 \geq \cdots ,$$

πράγμα που συμπεραίνουμε από το (ii) και (iii). Η αλυσίδα αυτή είναι τελικά σταθερή γιατί κάθε γνήσιο υποπρότυπο του $M$ έχει πεπερασμένο πλήθος υποπρότυπα όπως φαίνεται από τις (ii) και (iii). Άρα το $M$ είναι πρότυπο του Artin. Από το (iii) δεν είναι πρότυπο της Noether. □

## 5.2 Ιδιότητες

**5.2.1 Πρόταση** *Έστω*

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

*μια ακριβής ακολουθία R-προτύπων. Τότε*

*(i) Το $M$ είναι πρότυπο της Noether αν και μόνο αν τα $L$ και $N$ είναι πρότυπα της Noether.*

*(ii) Το $M$ είναι πρότυπο του Artin αν και μόνο αν τα $L$ και $N$ είναι πρότυποι του Artin.*

**Απόδειξη.** Θα αποδείξουμε το (i) μόνο καθώς η απόδειξη του (ii) είναι παρόμοια.

Έστω ότι το $M$ είναι της Noether. Θεωρούμε αύξουσα αλυσίδα υποπροτύπων του $L$

$$L_1 \subseteq L_2 \subseteq \cdots, \tag{1}$$

και αύξουσα αλυσίδα υποπροτύπων του $N$

$$N_1 \subseteq N_2 \subseteq \cdots. \tag{2}$$

Από την (1) παίρνουμε την αύξουσα ακολουθία υποπροτύπων του $M$,

$$f(L_1) \subseteq f(L_2) \subseteq \cdots \tag{3}$$

και από την (i) παίρνουμε την αύξουσα ακολουθία υποπροτύπων του $M$

$$g^{-1}(N_1) \subseteq g^{-1}(N_2) \subseteq \cdots. \tag{4}$$

Αφού ο $M$ είναι της Noether, η (3) είναι τελικά σταθερή. Επειδή ο $f$ είναι μονομορφισμός, συμπεραίνουμε ότι η (1) είναι τελικά σταθερή. Όμοια η (4) είναι τελικά σταθερή. Επειδή ο $g$ είναι επιμορφισμός, συμπεραίνουμε ότι η (2) είναι τελικά σταθερή.

Έστω, αντίστροφα, ότι τα $L$ και $N$ είναι πρότυπα της Noether. Έστω αύξουσα ακολουθία υποπροτύπων του $M$

$$M_1 \subseteq M_2 \subseteq \cdots.$$

Θεωρούμε την αύξουσα ακολουθία υποπροτύπων του $L$

$$f^{-1}(M_1) \subseteq f^{-1}(M_2) \subseteq \cdots$$

και την αύξουσα ακολουθία υποπροτύπων του $N$

$$g(M_1) \subseteq g(M_2) \subseteq \cdots.$$

Αυτές είναι τελικά σταθερές. Επομένως υπάρχει $n \in \mathbb{N}$ με την ιδιότητα

$$f^{-1}(M_n) = f^{-1}(M_{n+1}) = \cdots$$

και

$$g(M_n) = g(M_{n+1}) = \cdots.$$

Θα δείξουμε ότι $M_n = M_{n+1} = \cdots$. Έστω $x \in M_{k+1}$, όπου $k \geq n$. Τότε $g(x) \in g(M_{k+1}) = g(M_k)$. Άρα $g(x) = g(y)$ για κάποιο $y \in M_k$. Συνεπώς $g(x-y) = 0 \Rightarrow x - y \in \ker g = \text{Im } f \Rightarrow x - y \in \text{Im } f \cap M_{k+1} \Rightarrow f^{-1}(x-y) \in f^{-1}(M_{k+1}) = f^{-1}(M_k) \Rightarrow x - y \in M_k \Rightarrow x \in M_k$. Άρα $M_{k+1} \subseteq M_k$ και συνεπώς $M_{k+1} = M_k$. □

**5.2.2. Πόρισμα** *Έστω $M_1,...,M_n$ R-πρότυπα και M το ευθύ άθροισμά τους, $M = \overset{n}{\underset{i=1}{\oplus}} M_i$. Τότε*

*(i) Το M είναι της Noether αν και μόνο αν κάθε $M_i$ είναι της Noether.*

*(ii) Το M είναι του Artin αν και μόνο αν κάθε $M_i$ είναι του Artin.*

**Απόδειξη.** Θα δείξουμε το (i) μόνο καθώς η απόδειξη του (ii) είναι παρόμοια. Επαγωγή στο *n*. Για $n = 1$, το πόρισμα είναι προφανές. Έστω $n > 1$ και ότι το πόρισμα ισχύει για $n-1$ προσθετέους. Θεωρούμε την ακριβή ακολουθία

$$0 \to M_1 \xrightarrow{f} M_1 \oplus M_2 \oplus \cdots \oplus M_n \xrightarrow{g} M_2 \oplus \cdots \oplus M_n \to 0$$

όπου $f(x_1) = (x_1,0,...,0)$ και $g(x_1,...,x_n) = (x_2,...,x_n)$, $x_i \in M_i$. Από την Πρόταση 5.2.1, το $M_1 \oplus \cdots \oplus M_n$ είναι της Noether. Από την επαγωγική υπόθεση, το $M_2 \oplus \cdots \oplus M_n$ είναι της Noether αν και μόνο αν κάθε $M_2,...,M_n$ είναι της Noether. □

**5.2.3 Πόρισμα** *i) Έστω R δακτύλιος της Noether. Τότε κάθε πεπερασμένα παραγόμενο R-πρότυπο είναι της Noether.*

*ii) Έστω R δακτύλιος του Artin. Τότε κάθε πεπερασμένα παραγόμενο R-πρότυπο είναι του Artin.*

**Απόδειξη.** Πάλι θα δείξουμε μόνο το i). Έστω *M* πεπερασμένα παραγόμενο *R*-πρότυπο. Τότε (Πρόταση 3.4.2) υπάρχει επιμορφισμός $F \to M$, όπου το *F* είναι ελεύθερο *R*-πρότυπο με πεπερασμένη τάξη. Από τις Προτάσεις 3.4.2 και 5.2.2 και την υπόθεση συμπεραίνουμε ότι το *F* είναι πρότυπο της Noether. Από την Πρόταση 5.2.1 συμπεραίνουμε ότι το *M* είναι πρότυπο της Noether. □

**5.2.4 Παρατήρηση** 1) Η υπόθεση "πεπερασμένα παραγόμενο" στην προηγούμενη πρόταση είναι απαραίτητη. Για παράδειγμα το $k$-πρότυπο $k[x]$ ($k$ σώμα) δεν είναι ούτε της Noether ούτε του Artin αν και το $k$ είναι δακτύλιος και της Noether και του Artin.

2) Έστω $M$ ένα $R$-πρότυπο και $I$ ένα ιδεώδες του $R$ με την ιδιότητα $I \subseteq \operatorname{Ann} M$, δηλαδή $IM = 0$. Τότε ο $M$ έχει τη δομή $R/I$-προτύπου (Άσκηση 3.12). Ισχύει: το $M$ ως $R$-πρότυπο είναι της Noether (αντίστοιχα, του Artin) αν και μόνο αν είναι της Noether (αντίστοιχα, του Artin) ως $R/I$-πρότυπο, γιατί τα $R$-υποπρότυπα του $M$ και τα $R/I$ υποπρότυπα του $M$ ταυτίζονται. Αυτή η "αλλαγή δακτυλίων" είναι πολύ χρήσιμη όπως θα φανεί στη μεθεπομένη πρόταση.

**5.2.5 Πρόταση** *Έστω $k$ σώμα και $V$ ένας $k$-διανυσματικός χώρος. Οι παρακάτω συνθήκες είναι ισοδύναμες.*

*(i) Το $V$ έχει πεπερασμένη διάσταση*

*(ii) Το $V$ είναι $k$-πρότυπο της Noether*

*(iii) Το $V$ είναι $k$-πρότυπο του Artin.*

**Απόδειξη.** Άσκηση. □

Στο επόμενο κεφάλαιο η παρακάτω πρόταση θα χρησιμοποιηθεί δύο φορές.

**5.2.6 Πρόταση** *Έστω $R$ ένας δακτύλιος στον οποίο υπάρχουν μέγιστα ιδεώδη $M_1,...,M_t$ (όχι αναγκαστικά διακεκριμένα) με την ιδιότητα*

$$M_1 M_2 \cdots M_t = 0 .$$

*Τότε ο $R$ είναι δακτύλιος της Noether αν και μόνο αν είναι δακτύλιος του Artin.*

**Απόδειξη.** Επαγωγή στο $t$. Για $t = 1$, έχουμε $M_1 = 0$ και άρα το $R$ είναι σώμα, επειδή το 0 είναι μέγιστο ιδεώδες. Προφανώς ισχύει η πρόταση. Έστω $t > 1$. Θεωρούμε την ακριβή ακολουθία

$$0 \to M_t \to R \to R/M_t \to 0 .$$

Από την Πρόταση 5.2.1, το $R$ είναι δακτύλιος της Noether αν και μόνο αν τα $M_t$ και $R/M_t$ είναι $R$-πρότυπα της Noether. Έχουμε $R/M_t$ είναι $R$-πρότυπο της Noether $\Leftrightarrow$ (Παρατήρηση 5.2.4 (2)) $R/M_t$ είναι $R/M_t$-πρότυπο του Artin $\Leftrightarrow$ (Παρατήρηση 5.2.4 (2)) $R/M_t$ είναι $R$-πρότυπο του Artin. Άρα αρκεί να δείξουμε ότι: $M_t$ είναι $R$-πρότυπο της Noether $\Leftrightarrow$ $M_t$ είναι $R$-πρότυπο του Artin.

Πιο γενικά θα αποδείξουμε για κάθε $k=1,...,t$ ότι το $R$-πρότυπο $M_k\cdots M_t$ είναι της Noether αν και μόνο αν είναι του Artin. Επαγωγή στο $k$. Για $k=1$, η υπόθεση δίνει $M_1\cdots M_t=0$. Έστω $k>1$. Θεωρούμε την ακριβή ακολουθία $R$-προτύπων

$$0\to M_k\cdots M_t\to M_{k+1}\cdots M_t\to M_{k+1}\cdots M_t/M_k\cdots M_t\to 0, \qquad (5)$$

όπου $M_k\cdots M_t=M_k(M_{k+1}\cdots M_t)\subseteq M_{k+1}\cdots M_t$. Το πηλίκο $M_{k+1}\cdots M_t/M_k\cdots M_t$ είναι $R/M_k$-πρότυπο. Συνδυάζοντας την Πρόταση 5.2.5 και την Παρατήρηση 5.2.4(2) έχουμε ότι το πηλίκο αυτό είναι $R$-πρότυπο της Noether αν και μόνο αν είναι $R$-πρότυπο του Artin. Από την επαγωγική υπόθεση, το ίδιο ισχύει για το $R$-πρότυπο $M_k\cdots M_t$. Τέλος η (5) και η Πρόταση 5.2.1 δίνει ότι το $M_{k+1}\cdots M_t$ είναι της Noether αν και μόνο αν είναι του Artin. □

## 5.3 Συνθετικές σειρές

Έχοντας μελετήσει πρότυπα της Noether και πρότυπα του Artin είναι φυσικό να αναρωτηθούμε ποια πρότυπα είναι ταυτόχρονα και της Noether και του Artin. Εδώ εμφανίζεται η έννοια της συνθετικής σειράς.

**5.3.1 Ορισμός** *(i) Ένα $R$-πρότυπο λέγεται απλό αν δεν έχει μη μηδενικό γνήσιο υποπρότυπο.*

*(ii) Μια συνθετική σειρά μήκους $n$ του $R$-προτύπου $M$ είναι μία γνήσια φθίνουσα αλυσίδα υποπροτύπων μήκους $n$*

$$M=M_0\supsetneq M_1\supsetneq\cdots\supsetneq M_n=0 \qquad (1)$$

*τέτοια ώστε κάθε πηλίκο $M_i/M_{i+1}$ είναι απλό $R$-πρότυπο.*

Επειδή κάθε υποπρότυπο του $M_i / M_{i+1}$ είναι της μορφής $N / M_{i+1}$, όπου $M_{i+1} \leq N \leq M_i$, η αλυσίδα (1) είναι συνθετική σειρά αν δεν μπορεί να επιμηκυνθεί με την παρεμβολή άλλων υποπροτύπων.

Για παράδειγμα, κάθε συνθετική σειρά ενός *n*-διάστατου *k*-διανυσματικού χώρου *V* είναι μια ακολουθία υποχώρων

$$V = V_0 \supseteq V_1 \supseteq \cdots \supseteq V_n = 0,$$

όπου $\dim V_i = n - i$. Μια συνθετική σειρά του $\mathbb{Z}$-προτύπου $\mathbb{Z}_{12}$ είναι

$$\mathbb{Z}_{12} \supseteq <3> \supseteq <6> \supseteq 0,$$

και μία άλλη είναι

$$\mathbb{Z}_{12} \supseteq <2> \supseteq <6> \supseteq 0,$$

(γιατί;). Τα μήκη των δύο συνθετικών σειρών του $\mathbb{Z}_{12}$ συμπίπτουν. Αυτό δεν είναι τυχαίο:

**5.3.2 Πρόταση** *Έστω ότι το R-πρότυπο M έχει μια συνθετική σειρά μήκους n. Τότε κάθε άλλη συνθετική σειρά του M έχει μήκος n. Επιπλέον κάθε πεπερασμένη γνήσια φθίνουσα αλυσίδα υποπροτύπων του M μπορεί να επιμηκυνθεί σε συνθετική σειρά (με την παρεμβολή κάποιων υποπροτύπων).*

**Απόδειξη.** Αν *N* είναι ένα *R*-πρότυπο, με $\ell(N)$ συμβολίζουμε το ελάχιστο μήκος των συνθετικών σειρών του *N*. (Στην περίπτωση που το *N* δεν έχει συνθετική σειρά, ορίζουμε $\ell(N) = \infty$).

*Ισχυρισμός 1.* $N \subsetneq M \Rightarrow \ell(N) < \ell(M)$.

*Απόδειξη.* Έστω

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$$

συνθετική σειρά του *M* μήκους $n = \ell(N)$. Θεωρούμε την αλυσίδα υποπροτύπων

$$N = M_0 \cap N \supseteq M_1 \cap N \supseteq \cdots \supseteq M_n \cap N = 0 \qquad (2)$$

Για κάθε $i = 0,\ldots,n-1$ η απεικόνιση

$$\frac{M_i \cap N}{M_{i+1} \cap N} \to \frac{M_i}{M_{i+1}}, \quad x + M_{i+1} \cap N \mapsto x + M_{i+1} \qquad (3)$$

είναι επιμορφισμός *R*-προτύπων, γιατί ο πυρήνας της σύνθεσης $M_i \cap N \to M_i \to M_i / M_{i+1}$ είναι $M_i \cap N \cap M_{i+1} = M_{i+1} \cap N$. Όμως το $M_i / M_{i+1}$ είναι απλό. Άρα $M_i \cap N = M_{i+1} \cap N$ ή $M_i \cap N / M_{i+1} \cap N \cong M_i / M_{i+1}$.

Αν ισχύει η πρώτη περίπτωση, αφαιρούμε τον όρο $M_{i+1} \cap N$ από την αλυσίδα (2). Ό,τι μείνει είναι προφανώς συνθετική σειρά και έχει μήκος $< n$. Μένει να εξετάσουμε τι συμβαίνει αν για κάθε *I* ισχύει η δεύτερη περίπτωση. Από $M_i \cap \quad N / M_{i+1} \cap N \cong M_i / M_{i+1}$ για $i = n-1$ παίρνουμε $M_{n-1} \cap N = M_{n-1}$ (ισχύει = και όχι μόνο ≠ από τον ορισμό της (3)). Συνεχίζοντας κατά αυτόν τον τρόπο συμπεραίνουμε $M_{n-2} \cap N = M_{n-2}, ..., M_0 \cap N = M_0$, δηλαδή $M = N$.

*Ισχυρισμός 2.* Κάθε πεπερασμένη γνήσια φθίνουσα αλυσίδα υποπροτύπων

$$M = M'_0 \supsetneq M'_1 \supsetneq \cdots \supsetneq M'_k = 0$$

έχει μήκος $k \le \ell(N)$.

*Απόδειξη.* Από τον ισχυρισμό 1 έχουμε $\ell(M) > \ell(M'_1) > \cdots > \ell(M'_k) = 0$. Άρα $\ell(M) \ge k$.

Ερχόμαστε τώρα στην απόδειξη της πρότασης. Θεωρούμε μια συνθετική σειρά του *M* μήκους *k*. Τότε $k \le \ell(M)$ από τον ισχυρισμό 2. Αλλά από τον ορισμό του $\ell(M)$, έχουμε $k \ge \ell(M)$. Συνεπώς $k = \ell(M)$.

Έστω τέλος μια πεπερασμένη γνήσια φθίνουσα αλυσίδα υποπροτύπων του *M* μήκος *k*. Τότε $k \le \ell(M)$. Αν $k < \ell(M)$, τότε αυτή δεν είναι συνθετική σειρά, γιατί αποδείξαμε ότι δύο συνθετικές σειρές του *M* έχουν το ίδιο μήκος. Έτσι μπορούμε να παρεμβάλουμε όρους ώστε το μήκος της νέας ακολουθίας είναι $k' = \ell(M)$. Αλλά τότε η νέα ακολουθία είναι προφανώς συνθετική σειρά. □

**5.3.3 Θεώρημα** *Το R-πρότυπο M έχει συνθετική σειρά αν και μόνο αν είναι R-πρότυπο της Noether και του Artin.*

**Απόδειξη.** Έστω ότι το *M* έχει συνθετική σειρά. Από την Πρόταση 5.3.2 έπεται ότι σε κάθε (αύξουσα ή φθίνουσα) ακολουθία υποπροτύπων του *M* υπάρχουν το πολύ $\ell(M) < \infty$ γνήσιες διαδοχικές σχέσεις υποσυνόλου $\subsetneq$ ή $\supsetneq$. Αντίστροφα, έστω ότι το *M* είναι και της Noether και του Artin. Κατασκευάζουμε συνθετική

σειρά του $M$ κατά τον προφανή τρόπο: έστω $M_1$ μέγιστο υποπρότυπο του $M$ (υπάρχει τέτοιο γιατί το $M$ είναι της Noether), έστω $M_2$ μέγιστο υποπρότυπο του $M_1$ (το $M_1$ είναι της Noether από την Πρόταση 5.2.1), έστω $M_3$ μέγιστο υποπρότυπο του $M_2$, κ.ο.κ. Έχουμε

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots .$$

Επειδή το $M$ είναι του Artin, η παραπάνω ακολουθία τερματίζει στο 0 μετά από πεπερασμένο πλήθος βήματα. □

Το *μήκος*, $\ell(M) = \ell_R(M)$, ενός $R$-προτύπου $M$ είναι το μήκος μιας συνθετικής σειράς, αν υπάρχει τέτοια, διαφορετικά είναι $\infty$. Άρα $\ell(M) < \infty$ αν και μόνο αν το $M$ είναι και της Noether και του Artin.

## Ασκήσεις

**1.** (i) Έστω $f : M \to M$ επιμορφισμός $R$-προτύπων, όπου το $M$ είναι πρότυπο της Noether. Τότε ο $f$ είναι ισομορφισμός.

(ii) Έστω $g : N \to N$ μονομορφισμός $R$-προτύπων, όπου το $N$ είναι πρότυπο του Artin. Τότε ο $g$ είναι ισομορφισμός

(Υπόδειξη: (i) Θεωρήστε $\ker(f^n)$, (ii) θεωρήστε $M / \mathrm{Im}(g^n)$).

**2.** Έστω $N_1$, $N_2$ υποπρότυπα του $R$-προτύπου $M$. Αν τα $M / N_1$ και $M / N_2$ είναι της Noether (αντίστοιχα του Artin) τότε και το $M / N_1 \cap N_2$ είναι της Noether (αντίστοιχα του Artin).

**3.** Έστω $M$ ένα $R$-πρότυπο της Noether. Τότε ο δακτύλιος $R / \mathrm{Ann}\, M$ είναι της Noether. (Υπόδειξη: αν $M = < m_1, ..., m_k >$, τότε $\mathrm{Ann}\, M = \bigcap_i \mathrm{Ann} < m_i >$ και το $R / \mathrm{Ann}\, M$ εμφυτεύεται στο $\bigoplus_{i=1}^{k} R / \mathrm{Ann} < m_i > \cong \bigoplus_{i=1}^{k} < m_i >$).

**4.** Έστω $M$ πεπερασμένα παραγόμενο $R$-πρότυπο του Artin. Τότε ο δακτύλιος $R / \mathrm{Ann}\, M$ είναι του Artin.

**5.** Αληθεύει ότι το $\mathbb{Q}$ είναι $\mathbb{Z}$-πρότυπο της Noether; Του Artin;

**6.** Αν *I, J* είναι ιδεώδη του *R* με την ιδιότητα οι δακτύλιοι $R/I$ και $R/J$ είναι της Noether, αποδείξτε ότι το *R*-πρότυπο $R/I \oplus R/J$ είναι της Noether.

**7.** Έστω

$$0 \to L \to M \to N \to 0$$

ακριβής ακολουθία *R*-προτύπων. Τότε $\ell(M) < \infty$ αν και μόνο αν $\ell(L) < \infty$ και $\ell(N) < \infty$. Επιπλέον $\ell(M) = \ell(L) + \ell(N)$.

**8.** Ποιο είναι το $\ell(M)$, όπου είναι το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_{20} \oplus \mathbb{Z}_{27}$;

**9.** Θυμηθείτε το θεώρημα Jordan-Hölder από τις πεπερασμένες ομάδες. Διατυπώστε ένα ανάλογο θεώρημα για πρότυπα πεπερασμένου μήκους. Βεβαιωθείτε ότι η ίδια απόδειξη ισχύει και εδώ!

**10.** Έστω *M* ένα *R*-πρότυπο με $\ell(M) < \infty$ και έστω *N* ένα υποπρότυπο του *M*. Αν $\ell(N) = \ell(M)$ τότε $N = M$.

**11.** Έστω *M* ένα *R*-πρότυπο με $\ell(M) < \infty$ και $N_1$, $N_2$ υποπρότυπα του *M*. Τότε $\ell(N_1 + N_2) = \ell(N_1) + \ell(N_2) - \ell(N_1 \cap N_2)$. Τι σας θυμίζει αυτή η ισότητα; (Υπόδειξη: άσκηση 7).

**12.** Έστω *k* σώμα και $m \geq 1$. Τότε ο δακτύλιος $k[x]/(x^m)$ είναι του Artin. Ποιο γενικά, αν $f \in k[x]$ με $f \neq 0$ τότε ο δακτύλιος $k[x]/(f)$ είναι του Artin. Γενικεύσατε ακόμα περισσότερο με τυχαία περιοχή κυρίων ιδεωδών στη θέση του $k[x]$. Ισχύει η γενίκευσή σας για περιοχές μοναδικής παραγοντοποίησης;

# Κεφάλαιο 6

# Δακτύλιοι του Artin

Χρησιμοποιώντας τα αποτελέσματα του προηγούμενου κεφαλαίου θα αποδείξουμε εδώ ότι κάθε δακτύλιος του Artin είναι και δακτύλιος της Noether, ένα αποτέλεσμα που μάλλον δεν χαρακτηρίζεται ως αναμενόμενο. Επιπλέον θα μελετήσουμε τη δομή των δακτυλίων του Artin τόσο, όσο χρειάζεται να επισημάνουμε την ειδοποιό διαφορά τους με τους δακτύλιους της Noether: ένας δακτύλιος της Noether είναι δακτύλιος του Artin αν και μόνο αν κάθε πρώτο ιδεώδες είναι μέγιστο (Θεώρημα 6.2.5).

Στο πρώτο μέρος του κεφαλαίου αυτού θα ασχοληθούμε με μερικά χαρακτηριστικά αποτελέσματα που αφορούν ριζικά ιδεωδών σε γενικούς δακτύλιους που θα εφαρμοστούν και σε επόμενα κεφάλαια.

## 6.1 Ριζικό Ιδεώδους

**6.1.1 Ορισμός** *Έστω $I$ ένα ιδεώδες του $R$. Το ριζικό του είναι το ιδεώδες του $R$*

$$\operatorname{rad} I = \sqrt{I} = \{r \in R \mid r^n \in I \quad \text{για κάποιο} \quad n \in \mathbb{N}\}.$$

Το $\sqrt{I}$ είναι πράγματι ιδεώδες: αν $r, s \in \sqrt{I}$ τότε $r^m \in I$ και $s^n \in I$ για κάποια $m, n \in \mathbb{N}$. Θέτοντας $k = m + n$ έχουμε

$$(r+s)^k = \sum_i \binom{k}{i} r^i s^{k-i}.$$

Αν $i \geq m$, τότε $r \in I$ και άρα $r^i s^{k-i} \in I$. Αν $i < m$, τότε $k - i \geq n$ και άρα $s^{k-i} \in I$ οπότε $r^i s^{k-i} \in I$. Άρα σε κάθε περίπτωση $(r+s)^k \in I$, δηλαδή $r + s \in \sqrt{I}$. Αν $a \in R$, τότε $(ar)^m = a^m r^m \in I$. Άρα $ar \in I$.

Για παράδειγμα, αν το $P$ είναι πρώτο ιδεώδες του $R$, τότε $\sqrt{P} = P$. Το ριζικό του ιδεώδους (12) του $\mathbb{Z}$ είναι το (6) (γιατί;). Το ριζικό του $(x^2y^3)$ στο $\mathbb{Z}[x, y]$ είναι $(xy)$.

Το ριζικό του μηδενικού ιδεώδους αποτελείται προφανώς από τα μηδενοδύναμα στοιχεία του δακτυλίου, $\sqrt{0} = \{r \in R \mid r^n = 0 \text{ για κάποιο } n \in N\}$.

**6.1.2 Πρόταση** *Έστω $I$ ένα ιδεώδες του $R$. Τότε έχουμε*

$$\sqrt{I} = \bigcap_{\substack{P \supseteq I \\ P \text{ πρώτο}}} P$$

*δηλαδή το $\sqrt{I}$ είναι η τομή των πρώτων ιδεωδών του $R$ που περιέχουν το $I$. Ειδικότερα*

$$\sqrt{0} = \bigcap_{P \text{ πρώτο}} P .$$

**Απόδειξη.** Έστω $r \in \sqrt{I}$. Τότε $r^n \in I$. Αν $P$ είναι πρώτο ιδεώδες με $I \in P$, τότε $r^n \in P$ και άρα $r \in P$.

Για την άλλη σχέση, έστω (για άτοπο) $a \in \bigcap_{\substack{P \supseteq I \\ P \text{ πρώτο}}} P$ με $a \notin \sqrt{I}$.

Το σύνολο $S = \{a^m \mid m \in N\}$ είναι πολλαπλασιαστικό και ισχύει $S \cap I = \varnothing$, γιατί $a \notin \sqrt{I}$. Σύμφωνα με την Πρόταση 3.5.4 υπάρχει πρώτο ιδεώδες $P'$ του $R$ με την ιδιότητα $P' \supseteq I$ και $P' \cap I = \varnothing$. Αλλά $a \in P'$ και $a \in S$ που είναι άτοπο. □

Το παρακάτω λήμμα δεν έχει σχέση με ριζικά αλλά θα χρησιμοποιηθεί στα επόμενα.

**6.1.3 Λήμμα** *Έστω $I_1, ..., I_n$, $P$ ιδεώδη του $R$ με $P$ πρώτο. Τότε*

*(i)* $I_1 I_2 \cdots I_n \subseteq P \Leftrightarrow I_k \subseteq P$ *για κάποιο $k$*

*(ii)* $P = I_1 \cap \cdots \cap I_n \Rightarrow P = I_k$ *για κάποιο $k$.*

**Απόδειξη.** (i) Αν $I_k \subseteq P$, τότε $I_1 I_2 \cdots I_n \subseteq I_k \subseteq P$. Έστω $I_1 I_2 \cdots I_n \subseteq P$. Αν για κάθε $i = 1,2,...,n$ είχαμε $I_i \not\subseteq P$ τότε θα υπήρχαν $a_i \in I_i - P$, οπότε το $a_1 a_2 \cdots a_n \in I_1 I_2 \cdots I_n \subseteq P$, άτοπο γιατί το $P$ είναι πρώτο.

(ii) Έχουμε $I_1 I_2 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n = P$. Άρα $I_k \subseteq P$ για κάποιο $k$ από το (i), οπότε $I_k = P$. □

Επίσης θα χρειαστούμε το επόμενο λήμμα.

**6.1.4 Λήμμα** *Έστω R ένας δακτύλιος της Noether και I ένα ιδεώδες του R. Τότε υπάρχει* $t \in \mathbb{N}$ *με την ιδιότητα* $(\sqrt{I})^t \subseteq I$.

**Απόδειξη.** Το $\sqrt{I}$ είναι πεπερασμένα παραγόμενο γιατί ο $R$ είναι της Noether. Έστω

$$\sqrt{I} = (a_1,...,a_r).$$

Για κάθε $a_i$, υπάρχει $n_i \in \mathbb{N}$ με την ιδιότητα $a_i^{n_i} \in I$. Θέτουμε

$$t = 1 + \sum_{i=1}^{r} (n_i - 1).$$

Το $(\sqrt{I})^t$ παράγεται προφανώς από το σύνολο

$$\left\{ a_i^{t_1} \cdots a_r^{t_r} \mid \sum t_i = t \right\}.$$

Όμως, αν

$$\sum_{i=1}^{r} t_i = t = 1 + \sum_{i=1}^{r} (n_i - 1),$$

τότε για κάποιο $t_j$ ισχύει $t_j \geq n_j$. Κατά συνέπεια

$$a_i^{t_1} \cdots a_j^{t_j} \cdots a_r^{t_r} \in I.$$

Άρα $(\sqrt{I})^t \subseteq I$. □

## 6.2 Δακτύλιοι του Artin είναι Δακτύλιοι της Noether

Οι επόμενες δύο προτάσεις δείχνουν ότι οι δακτύλιοι του Artin έχουν "λίγα" πρώτα ιδεώδη.

**6.2.1 Πρόταση** *Έστω R δακτύλιος του Artin. Τότε κάθε πρώτο ιδεώδες του R είναι και μέγιστο.*

**Απόδειξη.** Έστω $P$ πρώτο ιδεώδες του $R$. Τότε ο $R/P$ είναι δακτύλιος του Artin (Πρόταση 5.2.1) και περιοχή (Πρόταση 0.6.2). Θα δείξουμε ότι ο $R/P$ είναι σώμα. Έστω $r \in R/P$ με $r \neq 0$. Τότε η ακολουθία ιδεωδών του $R/P$

$$(r) \supseteq (r^2) \supseteq (r^3) \supseteq \cdots$$

είναι τελικά σταθερή, οπότε $r^n = sr^{n+1}$ για κάποια $n \in \mathbb{N}$ και $s \in R/P$. Άρα $r^n(1-sr) = 0$, και εφόσον βρισκόμαστε σε περιοχή ισχύει $1-sr$. Άρα το $r$ είναι αντιστρέψιμο. □

**6.2.2 Πρόταση** *Το πλήθος των μέγιστων ιδεωδών κάθε δακτύλιου του Artin είναι πεπερασμένο.*

**Απόδειξη.** Θεωρούμε το σύνολο $\Omega = \{M_1 \cap \cdots \cap M_t \mid t \in \mathbb{N},\ M_i$ μέγιστο ιδεώδες του $R$ για κάθε $i = 1,...,t\}$. Είναι $\Omega \neq \varnothing$ (γιατί;) και αφού ο $R$ είναι του Artin, το $\Omega$ έχει ελάχιστο στοιχείο, έστω

$$I = M_1 \cap \cdots \cap M_n.$$

Θα δείξουμε ότι κάθε μέγιστο ιδεώδες του $R$ είναι ένα από τα $M_1,...,M_n$. Έστω λοιπόν $M$ μέγιστο ιδεώδες. Τότε

$$M \cap M_1 \cap \cdots \cap M_n \subseteq I\ .$$

Από τον ορισμό του $I$ έχουμε

$$M \cap M_1 \cap \cdots \cap M_n = I$$

και συνεπώς

$$M \cap (M_1 \cap \cdots \cap M_n) = M_1 \cap \cdots \cap M_n\ .$$

Άρα $M_1 \cap \cdots \cap M_n \subseteq M$. Από την Πρόταση 6.3.1 (i) παίρνουμε $M_k \subseteq M$ για κάποιο $k = 1,...,n$. Το $M_k$ είναι μέγιστο και έχουμε $M \neq R$). Άρα $M_k = M$. □

**6.2.3 Πρόταση** *Έστω R δακτύλιος του Artin. Τότε υπάρχει $n \in \mathbb{N}$ με την ιδιότητα*

$$(\sqrt{0})^n = 0\ .$$

**Απόδειξη.** Επειδή ο $R$ είναι του Artin, η αλυσίδα

$$\sqrt{0} \supseteq (\sqrt{0})^2 \supseteq \cdots$$

είναι τελικά σταθερή, δηλαδή $(\sqrt{0})^n = (\sqrt{0})^{n+1} = \cdots$. Θα δείξουμε ότι

$$(\sqrt{0})^n = 0 . \tag{1}$$

Έστω ότι δεν ισχύει η (1). Θα καταλήξουμε σε άτοπο. Έστω

$$\Omega = \{I \text{ ιδεώδες του } R \mid I(\sqrt{0})^n \neq 0\} .$$

Τότε $\Omega \neq \varnothing$ αφού $R \in \Omega$. Επειδή ο $R$ είναι του Artin, το $\Omega$ έχει ελάχιστο στοιχείο, έστω $J$.

Το $J$ είναι κύριο ιδεώδες. Πράγματι, υπάρχει $a \in J$ με την ιδιότητα $a(\sqrt{0})^n \neq 0$, γιατί $J(\sqrt{0})^n \neq 0$. Άρα $(a)(\sqrt{0})^n \neq 0$, δηλαδή $(a) \in \Omega$. Επειδή $(a) \subseteq J$, ο ορισμός του $J$ δίνει $J = (a)$.

Ισχυριζόμαστε ότι $a(\sqrt{0})^n = J$. Πράγματι, έχουμε

$$a(\sqrt{0})^n(\sqrt{0})^n = a(\sqrt{0})^{2n} = a(\sqrt{0})^n = J(\sqrt{0})^n \neq 0 ,$$

και άρα $a(\sqrt{0})^n \in \Omega$. Επειδή $a(\sqrt{0})^n \subseteq J$, παίρνουμε όπως και πριν ότι $a(\sqrt{0})^n = J$.

Η τελευταία σχέση δίνει $a = ab$ για κάποιο $b \in (\sqrt{0})^n$. Τότε $a = ab = ab^2 = ab^3 = \cdots$. Αλλά $b \in (\sqrt{0})^n \subseteq \sqrt{0}$. Συνεπώς $b^k = 0$ για κάποιο $k$. Άρα $a = ab^k = 0$. Συνεπώς $J = 0$, που είναι άτοπο από τον ορισμό του $J$. □

Είμαστε τώρα σε θέση να αποδείξουμε το πρώτο από τα δύο κύρια αποτελέσματα αυτού του κεφαλαίου.

**6.2.4 Θεώρημα** *Κάθε δακτύλιος του Artin είναι δακτύλιος της Noether.*

**Απόδειξη.** Έστω $R$ ένας δακτύλιος του Artin. Από την Πρόταση 6.1.2 έχουμε

$$\sqrt{0} = \bigcap_{P \text{ πρώτο}} P .$$

Όμως από την Πρόταση 6.2.1 κάθε πρώτο ιδεώδες είναι μέγιστο. Επιπλέον, η Πρόταση 6.2.2 μας πληροφορεί ότι τα μέγιστα ιδεώδη του $R$ είναι πεπερασμένα στο πλήθος. Άρα

$$\sqrt{0} = M_1 \cap \cdots \cap M_n \qquad (2)$$

όπου $M_1,...,M_n$ είναι όλα τα μέγιστα ιδεώδη του $R$. Η (2) σε συνδυασμό με την Πρόταση 6.2.3 δίνει: υπάρχει $m \in \mathbb{N}$ τέτοιο ώστε

$$(M_1 \cap \cdots \cap M_n)^m = 0 . \qquad (3)$$

Επειδή $M_1 M_2 \cdots M_n \subseteq M_1 \cap \cdots \cap M_n$, η (3) δίνει

$$M_1^m \cdots M_n^m = 0 .$$

Τότε εφαρμόζουμε την Πρόταση 5.2.6 για να συμπεράνουμε ότι ο $R$ είναι δακτύλιος της Noether. □

Προφανώς δεν ισχύει το αντίστροφο του Θεωρήματος 6.2.4 (Παράδειγμα 5.1.5 (1)). Μπορούμε όμως να χαρακτηρίσουμε τους δακτυλίους της Noether που είναι και δακτύλιοι του Artin με το παρακάτω κομψό αποτέλεσμα.

**6.2.5 Θεώρημα** *Έστω R ένας δακτύλιος. Τότε το R είναι του Artin αν και μόνο αν είναι της Noether και κάθε πρώτο ιδεώδες είναι μέγιστο.*

Η απόδειξη θα δοθεί στην επόμενη παράγραφο, γιατί απαιτεί μια νέα έννοια. Ας προσπαθήσουμε εδώ να δώσουμε το κίνητρο.

Στην απόδειξη του Θεωρήματος 6.2.5 θα θέλαμε να δείξουμε ότι: Έστω $R$ δακτύλιος της Noether όπου κάθε πρώτο ιδεώδες είναι μέγιστο. Τότε $\sqrt{0} = M_1 \cap \cdots \cap M_n$ για μέγιστα ιδεώδη $M_1,...,M_n$ του $R$. (Αυτό αρκεί λόγω του Λήμματος 6.1.4 και της Πρότασης 5.2.6).

Έχουμε (Άσκηση 4.3)

$$\sqrt{0} = I_1 \cap \cdots \cap I_k , \quad I_i \quad \text{ανάγωγο.}$$

Μπορούμε να δείξουμε ότι (θα το δούμε παρακάτω)

$$\sqrt{I_i} = \text{πρώτο} = \text{μέγιστο ιδεώδες.} \qquad (5)$$

Τώρα χρησιμοποιώντας απλές ιδιότητες του ριζικού παίρνουμε

$$\sqrt{0} = \sqrt{\sqrt{0}} = \sqrt{I_1 \cap \cdots \cap I_k} = \sqrt{I_1} \cap \cdots \cap \sqrt{I_k} ,$$

και άρα προκύπτει το ζητούμενο

$$\sqrt{0} = M_1 \cap \cdots \cap M_k .$$

Το κρίσιμο σημείο είναι η πρώτη ισότητα της (5). Άρα εύλογο είναι να θεωρήσουμε ιδεώδη $I$ με την ιδιότητα $\sqrt{I}$ είναι πρώτο ιδεώδες. Μια κλάση τέτοιων ιδεωδών είναι τα πρωταρχικά ιδεώδη με τον ορισμό των οποίων αρχίζει η επόμενη παράγραφος.

## 6.3 Πρωταρχικά Ιδεώδη

**6.3.1 Ορισμός** *Ένα γνήσιο ιδεώδες $I$ του $R$ λέγεται πρωταρχικό αν $xy \in I \Rightarrow$ είτε $x \in I$ είτε $y^n \in I$ για κάποιο $n \in \mathbb{N}$.*

Για παράδειγμα κάθε πρώτο ιδεώδες είναι πρωταρχικό. Το ιδεώδες $(p^n)$ του $\mathbb{Z}$ ($p$ πρώτος) είναι πρωταρχικό, ενώ το $(pq)$ ($p \neq q$ πρώτοι) δεν είναι.

**6.3.2 Πρόταση** *$I$ πρωταρχικό $\Rightarrow \sqrt{I}$ πρώτο ιδεώδες. Το αντίστροφο δεν ισχύει.*

**Απόδειξη.** $xy \in \sqrt{I} \Rightarrow x^n y^n \in I \Rightarrow x^n \in I$ ή $y^{nm} \in I$ για κάποιο $m \in \mathbb{N} \Rightarrow x \in \sqrt{I}$ ή $y \in \sqrt{I}$. Για το αντίστροφο, ένα αντιπαράδειγμα είναι $R = k[x, y]$ (δακτύλιος πολυωνύμων), $I = (x^2, xy)$. Τότε $\sqrt{I} = (x)$ που είναι πρώτο ιδεώδες, αλλά το $I$ δεν είναι πρωταρχικό γιατί $xy \in I$ και $x \notin I$, $y \notin \sqrt{I}$. □

Θυμίζουμε ότι ένα ιδεώδες $I$ του $R$ λέγεται *ανάγωγο* αν

$$I = I_1 \cap I_2 \Rightarrow I_1 = I \quad \text{ή} \quad I_2 = I$$

(Άσκηση 4.3).

**6.3.3 Πρόταση** *Έστω ένας $R$ δακτύλιος της Noether. Τότε κάθε ανάγωγο ιδεώδες του $R$ είναι πρωταρχικό.*

**Απόδειξη.** Έστω $I$ ανάγωγο ιδεώδες και $xy \in I$ με $y \notin I$. Θα δείξουμε ότι $x^n \in I$ για κάποιο $n \in \mathbb{N}$.

Η αύξουσα αλυσίδα ιδεωδών του $R$

$$(I : x) \subseteq (I : x^2) \subseteq \cdots$$

είναι τελικά σταθερή, δηλαδή $(I : x^n) = (I : x^{n+1})$ για κάποιο $n \in \mathbb{N}$.

*Ισχυρισμός:* $I = (I + (x^n)) \cap (I + (y))$

*Απόδειξη.* Η σχέση $I \subseteq (I + (x^n)) \cap (I + (y))$ είναι προφανής. Έστω

$$r \in (I + (x^n)) \cap (I + (y)).$$

Τότε

$$r = g + cx^n = h + db$$

για κάποια $g, h \in I$ και $c, d \in R$. Γράφουμε

$$cx^{n+1} = hx + dxb - gx \in I.$$

Επομένως

$$c \in (I : x^{n+1}).$$

Άρα $c \in (I : x^n)$. Αλλά τότε $r = g + cx^n \in I$. Συνεπώς αποδείξαμε τον ισχυρισμό.

Από τον ισχυρισμό, το γεγονός ότι το $I$ είναι ανάγωγο και το γεγονός ότι $I \subsetneq I + (y)$, παίρνουμε $I = I + (x^n)$. Άρα $x^n \in I$. □

Περισσότερα για πρωταρχικά ιδεώδη θα πούμε στο Κεφάλαιο 11. Τώρα θα αποδείξουμε το Θεώρημα 6.2.5.

**Απόδειξη του Θεωρήματος 6.2.5.** 1) Έστω $R$ ένας δακτύλιος του Artin. Λόγω της Πρότασης 6.2.1 και του Θεωρήματος 6.2.4 δεν έχουμε να δείξουμε τίποτα.

2) Αντίστροφα, έστω $R$ ένας δακτύλιος της Noether όπου κάθε πρώτο ιδεώδες είναι μέγιστο. Αν $R = \{0\}$, δεν χρειάζεται να δείξουμε τίποτα. Έστω $R \neq \{0\}$. Τότε $1 \notin \sqrt{0}$, δηλαδή το ιδεώδες $\sqrt{0}$ είναι γνήσιο. Εφαρμόζοντας την Άσκηση 4.3 στο $\sqrt{0}$ παίρνουμε

$$\sqrt{0} = I_1 \cap \cdots \cap I_n$$

όπου τα $I_1, ..., I_n$ είναι ανάγωγα ιδεώδη του $R$. Εφαρμόζοντας στοιχειώδεις ιδιότητες του ριζικού (Άσκηση 1) έχουμε

$$\sqrt{0} = \sqrt{\sqrt{0}} = \sqrt{I_1 \cap \cdots \cap I_k} = \sqrt{I_1} \cap \cdots \cap \sqrt{I_k}.$$

Από την Πρόταση 6.3.3 κάθε $I_j$ είναι πρωταρχικό και συνεπώς από την Πρόταση 6.3.2 κάθε $\sqrt{I_j}$ είναι πρώτο ιδεώδες και άρα μέγιστο. Έχουμε δηλαδή

$$\sqrt{0} = M_1 \cap \cdots \cap M_n \quad (4) \tag{4}$$

όπου $M_1,...,M_n$ είναι μέγιστα ιδεώδη. Από την Πρόταση 6.1.4 έχουμε $(\sqrt{0})^t = 0$ για κάποιο $t$. Άρα από την (4) παίρνουμε

$$M_1^t \cdots M_n^t = 0 .$$

Επειδή τώρα ο $R$ είναι της Noether, η Πρόταση 5.2.6 μας δίνει ότι ο $R$ είναι του Artin. □

## Ασκήσεις

**1.** Έστω $I$, $J$ ιδεώδη του $R$. Τότε

(i) $\sqrt{\sqrt{I}} = \sqrt{I}$

(ii) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = \sqrt{IJ}$

(iii) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$

(iv) $\sqrt{I} = R \Leftrightarrow I = R$

(v) $\sqrt{I} + \sqrt{J} = R \Leftrightarrow I + J = R$

**2.** Έστω $R \neq \{0\}$. Τότε ο $R$ έχει ακριβώς ένα πρώτο ιδεώδες αν και μόνο αν κάθε στοιχείο του $R$ είναι είτε αντιστρέψιμο είτε μηδενοδύναμο.

**3.** Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων και έστω $Q$ ένα πρωταρχικό ιδεώδες στο $S$. Το $\varphi^{-1}(Q)$ είναι πρωταρχικό στο $R$;

**4.** Έστω $p$ πρώτος αριθμός και $n \geq 1$. Ο δακτύλιος $\mathbb{Z}/(p^n)$ είναι τοπικός δακτύλιος του Artin. (Τοπικός λέγεται ένας δακτύλιος που έχει ακριβώς ένα μέγιστο ιδεώδες). Επίσης τοπικός δακτύλιος του Artin είναι και ο $k[x^2, x^3]/(x^4)$ ($k$ σώμα).

**5.** Έστω $M$ μέγιστο ιδεώδες του δακτυλίου του Artin $R$. Τότε για κάθε $t \geq 1$ ο $R/M^t$ είναι τοπικός δακτύλιος του Artin (δες την προηγούμενη άσκηση για τον ορισμό του τοπικού δακτυλίου).

**6.** Ιδεώδη $I_1,...,I_n$ του $R$ λέγονται ανά δύο πρώτα αν $I_r + I_s = R$ για κάθε $r \neq s$. Αν τα $I_1,...,I_n$ είναι ανά δύο πρώτα, τότε $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.

**7.** Κάθε δακτύλιος του Artin είναι ισόμορφος με ευθύ γινόμενο πεπερασμένου πλήθους τοπικών δακτυλίων του Artin. (Υπόδειξη: Αν $M_1^t \cdots M_n^t = 0$, δείξετε ότι $A \cong A/M_1^t \times \cdots \times A/M_n^t$. Δες και τις Ασκήσεις 5, 6 και 1 (v)).

**8*.** Έστω $I$ ένα ιδεώδες του $R$ με την ιδιότητα ότι το $\sqrt{I}$ είναι μέγιστο ιδεώδες. Τότε το $I$ είναι πρωταρχικό. (Υπόδειξη: Έστω $ab \in I$ με $\sqrt{b} \notin I$. Τότε $\sqrt{I} + \sqrt{(b)} = R \Rightarrow$ (Άσκηση 1) $I + (b) = R$, οπότε $a = a \cdot 1 \in I$).

**9.** Ποιο είναι το ριζικό του ιδεώδους $(m)$ στο $\mathbb{Z}$; Ποια είναι τα πρωταρχικά ιδεώδη του $\mathbb{Z}$;

**10.** Έστω $A$ πρότυπο του Artin πάνω από το δακτύλιο $R$ και $a \in A$. Τότε υπάρχουν μέγιστα ιδεώδη $M_1,...,M_n$ του $R$ με την ιδιότητα

$$(M_1 \cdots M_n)^t a = 0.$$

(Υπόδειξη: Άσκηση 5.4).

**11.** Χωρίς να χρησιμοποιήσετε το Θεώρημα 6.2.5, αποδείξετε ότι σε ένα δακτύλιο της Noether, όπου κάθε πρώτο ιδεώδες είναι και μέγιστο, το πλήθος των μέγιστων ιδεωδών είναι πεπερασμένο (Υπόδειξη: για το $\sqrt{0}$ έχετε δύο παραστάσεις).

**12.** Έστω $R$ ένας δακτύλιος του Artin. Ποια $R$-πρότυπα έχουν πεπερασμένο μήκος;

**13.** Έστω $R$ ένας δακτύλιος της Noether και $I$, $J$ ιδεώδη του $R$. Τότε ισχύει $\sqrt{I} = \sqrt{J} \Leftrightarrow$ υπάρχει $n > 1$ με την ιδιότητα $I^n \in J$ και $J \subseteq I$.

**14.** Έστω $R = \mathbb{Z}[i]$ (ακέραιοι του Gauss) και $S = R[x]$ (πολυωνυμικός δακτύλιος). Τότε ο $S$ είναι δακτύλιος της Noether αλλά όχι του Artin.

# Κεφάλαιο 7

# Ακεραία Εξάρτηση και Κανονικοποίηση της Noether

Θα μελετήσουμε εδώ ακέραια στοιχεία πάνω από δακτύλιο. Αυτά συμπεριφέρονται κατά τρόπο ανάλογο με τα αλγεβρικά στοιχεία πάνω από σώμα, αλλά η μελέτη τους είναι κάπως πιο λεπτή.

Αφού αποδείξουμε βασικές ιδιότητες ακεραίων στοιχείων, προχωράμε αμέσως σε μια σημαντική εφαρμογή, το θεώρημα κανονικοποίησης της Noether. Αυτό θα χρησιμοποιηθεί στην απόδειξη του Nullstellensatz που δίνουμε στο Κεφάλαιο 8. Στο Κεφάλαιο 9 θα ακολουθήσουν εφαρμογές και άλλων προτάσεων από το παρόν κεφάλαιο.

Ξεκινάμε με μερικές χρήσιμες τεχνικές, όπως είναι το τέχνασμα της ορίζουσας και το Λήμμα του Nakayama.

## 7.1 Τέχνασμα της Ορίζουσας

Έστω $k$ ένα σώμα και $A$ ένας $n \times n$ πίνακας με στοιχεία από το $k$. Θυμίζουμε μια σημαντική σχέση οριζουσών από τη Γραμμική Άλγεβρα. Έστω $\tilde{A}_{ij}$ ο $(n-1)\times(n-1)$ πίνακας που προκύπτει από τον $A$ αν παραλείψουμε την $i$ γραμμή και $j$ στήλη. Θέτουμε $d_{ij} = (-1)^{i+j} \det(\tilde{A}_{ji})$. Ο $n \times n$ πίνακας $(d_{ij})$ συμβολίζεται με $adjA$ και ονομάζεται προσαρτημένος πίνακας του $A$. Ισχύει η σχέση

$$A(adjA) = (adjA) = (\det A) I_n, \tag{1}$$

όπου $I_n$ είναι ο ταυτοτικός $n \times n$ πίνακας.

Η σχέση (1) ισχύει πιο γενικά όταν αντικαταστήσουμε το σώμα $k$ με ένα (μεταθετικό, όπως πάντα) δακτύλιο $R$. Μάλιστα η κλασσική απόδειξη της (1) που συνήθως δίνεται στη Γραμμική Άλγεβρα ισχύει και για το $R$, οπότε δεν χρειάζεται να την επαναλάβουμε εδώ.

Αν $\varphi : R \to S$ είναι ένας ομομορφισμός δακτυλίων τότε κάθε $S$-πρότυπο $M$ μπορεί να θεωρηθεί ως $R$-πρότυπο με εξωτερικό πολλαπλασιασμό

$$rm = \varphi(r)m, \quad r \in R, \quad m \in M,$$

(Παράδειγμα 3.1.2 (v)). Συχνά στο κεφάλαιο αυτό θα έχουμε $R \subseteq S$ (ο $R$ είναι υποδακτύλιος του $S$), οπότε κάθε $S$-πρότυπο είναι $R$-πρότυπο κατά τον προφανή τρόπο.

Θα γράφουμε απλά $R \subseteq S$ εννοώντας ότι $R$ είναι υποδακτύλιος του $S$, και $M \in {}_S M$ εννοώντας ότι το $M$ είναι ένα $S$-πρότυπο.

**7.1.1 Πρόταση** *Έστω δακτύλιοι $R \subseteq S$ και $M \in {}_S M$. Έστω $s \in S$ και $I$ ιδεώδες του $R$ με την ιδιότητα $sM \subseteq IM$. Αν ως $R$-πρότυπο το $M$ παράγεται από $n \geq 1$ στοιχεία, τότε υπάρχουν $a_i \in I^i$, $i = 1,...,n$, με την ιδιότητα*

$$s^n + a_1 s^{n-1} + \cdots + a_{n-1} s + a_n \in \mathrm{Ann}\,{}_S M .$$

**Απόδειξη.** (Τέχνασμα της ορίζουσας) Έστω ότι το $M$ παράγεται ως $R$-πρότυπο από τα $m_1,...,m_n$. Για κάθε $i$ έχουμε $sm_i \in IM$. Συνεπώς

$$\begin{aligned} sm_1 &= b_{11}m_1 + b_{12}m_2 + \cdots + b_{1n}m_n \\ &\cdots \\ sm_n &= b_{n1}m_1 + b_{n2}m_2 + \cdots + b_{nn}m_n \end{aligned}$$

για κάποια $b_{ij} \in I$. Γράφουμε τις προηγούμενες εξισώσεις ως

$$\begin{aligned} 0 &= (b_{11} - s)m_1 + b_{12}m_2 + \cdots + b_{1n}m_n \\ &\cdots \\ 0 &= b_{n1}m_1 + b_{n2}m_2 + \cdots + (b_{nn} - s)m_n \end{aligned} \qquad (2)$$

Έστω $A$ ο $n \times n$ πίνακας των συντελεστών των $m_i$ στο σύστημα (2). Τότε

$$0 = A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

και άρα

$$0 = (adjA)A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}.$$

Η τελευταία σχέση λόγω της (1) δίνει

$$0 = (\det A) I_n \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}. \qquad (3)$$

Άρα $(\det A) m_i = 0$ για κάθε $i$. Εφόσον τα $m_i$ παράγουν το $M$ έχουμε $(\det A) M = 0$. Η επιθυμητή σχέση προκύπτει τώρα αν αναπτύξουμε την ορίζουσα $\det A$. □

**7.1.2 Πόρισμα** *Έστω $M$ ένα πεπερασμένα παραγόμενο $R$-πρότυπο και $I$ ιδεώδες του $R$ με την ιδιότητα $M = IM$. Τότε υπάρχει $a \in I$ με την ιδιότητα $(1+a)M = 0$.*

**Απόδειξη.** Θέτουμε $S = R$ και $s = 1$ στην Πρόταση 7.1.1. □

Ένας δακτύλιος ονομάζεται *τοπικός* αν έχει ακριβώς ένα μέγιστο ιδεώδες. Έστω $\underline{m}$ μέγιστο ιδεώδες του $R$ (Πρόταση 3.4.2). Τότε ο $R$ είναι τοπικός αν και μόνο αν κάθε στοιχείο της μορφής $1+a$ με $a \in \underline{m}$ είναι αντιστρέψιμο. Πράγματι, έστω $R$ τοπικός. Αν το $1+a$ δεν ήταν αντιστρέψιμο θα έπρεπε να περιέχεται σε κάποιο μέγιστο ιδεώδες (Πόρισμα 3.5.3), δηλαδή στο $\underline{m}$. Αλλά $1+a \in \underline{m} \Rightarrow 1 \in \underline{m}$ άτοπο. Αντίστροφα, έστω ότι κάθε $1+a$ είναι αντιστρέψιμο όπου $a \in \underline{m}$. Έστω $\underline{m'} \neq \underline{m}$ άλλο μέγιστο ιδεώδες. Έχουμε $\underline{m} + \underline{m'} = R$ από τον ορισμό του μέγιστου ιδεώδους. Άρα $a + b = 1$ για κάποια $a \in \underline{m}$, $b \in \underline{m'}$. Τότε το $b = 1 - a$ είναι αντιστρέψιμο. Άρα $\underline{m'} = R$, άτοπο.

**7.1.3 Λήμμα** *Έστω $\underline{m}$ μέγιστο ιδεώδες του $R$. Τότε ο $R$ είναι τοπικός δακτύλιος αν και μόνον αν το $1+a$ είναι αντιστρέψιμο στοιχείο του $R$ για κάθε $a \in \underline{m}$.* □

**7.1.4 Πόρισμα** *(Λήμμα του Nakayama). Έστω $R$ τοπικός δακτύλιος με μέγιστο ιδεώδες $\underline{m}$ και $M$ πεπερασμένα παραγόμενο $R$-πρότυπο. Αν $M = \underline{m}M$ τότε $M = 0$.*

**Απόδειξη.** Από το Πόρισμα 7.1.2 έχουμε

$$(1+a)M = 0$$

για κάποιο $a \in \underline{m}$. Αλλά από το Λήμμα 7.1.3, το $1+a$ είναι αντιστρέψιμο. Συνεπώς $M = (1+a)^{-1}(1+a)M = 0$. □

**Σημείωση.** 1) Η υπόθεση ότι το $M$ είναι πεπερασμένα παραγόμενο στο Λήμμα του Nakayama είναι απαραίτητη (Άσκηση 11). 2) Μπορεί να αποδειχθεί το Λήμμα Nakayama χωρίς να χρησιμοποιηθεί η Πρόταση 7.1.1. (Άσκηση 8).

## 7.2 Ακέραια Εξάρτηση

Αν $k \subseteq K$ είναι σώματα, ένα στοιχείο $a \in K$ λέγεται *αλγεβρικό πάνω από το* $k$ αν είναι ρίζα μη μηδενικού πολυωνύμου $f(x) \in k[x]$. Μπορούμε βέβαια να υποθέσουμε ότι το $f(x)$ είναι μονικό.

Αν $R \subseteq S$ είναι δακτύλιοι, ένα στοιχείο $s \in S$ λέγεται *ακέραιο πάνω από το* $R$ αν είναι ρίζα μονικού πολυωνύμου $f(x) \in R[x]$. Εδώ όμως η υπόθεση ότι το $f(x)$ είναι μονικό περιπλέκει αρκετά τη θεωρία. Η έννοια του ακεραίου στοιχείου πάνω από δακτύλιο οδηγεί στο δακτύλιο των ακεραίων $\mathcal{O}_K$ ενός αριθμητικού σώματος $K$ που είναι το αντικείμενο του Κεφαλαίου 9. Εδώ θα ασχοληθούμε με μερικές γενικές αλλά χρήσιμες ιδιότητες ακεραίων στοιχείων.

Για παράδειγμα, κάθε στοιχείο του $R$ είναι ακέραιο πάνω από το $R$. Το $a = \dfrac{1+\sqrt{5}}{2}$ είναι ακέραιο πάνω από το $\mathbb{Z}$, γιατί η ρίζα του μονικού πολυωνύμου $x^2 - x - 1$. Όμως το $b = \dfrac{1+\sqrt{3}}{2}$ δεν είναι ακέραιο πάνω από το $\mathbb{Z}$ (γιατί;).

Χρήσιμη θα είναι η ακόλουθη απλή παρατήρηση.

**7.2.1 Λήμμα** *Έστω $R \subseteq S \subseteq T$ δακτύλιοι. Αν το $T$ είναι πεπερασμένα παραγόμενο $S$-πρότυπο και το $S$ είναι πεπερασμένα παραγόμενο $R$-πρότυπο, τότε το $T$ είναι πεπερασμένα παραγόμενο $R$-πρότυπο.*

**Απόδειξη.** Αν το $T$ ως $S$-πρότυπο παράγεται από τα

$$t_1, \ldots, t_n$$

και το $S$ παράγεται ως $R$-πρότυπο από τα

$$s_1,\dots,s_m,$$

τότε το $T$ παράγεται ως $R$-πρότυπο από τα στοιχεία

$$s_i t_j, \quad i=1,\dots,m \quad \text{και} \quad j=1,\dots,n. \qquad \square$$

Ένα $R$-πρότυπο $M$ λέγεται *πιστό* αν $\operatorname{Ann} M = 0$. Ακολουθεί τώρα μια πρόταση που θα βρει πολλές εφαρμογές.

**7.2.2 Πρόταση** *Έστω $R \subseteq S$ δακτύλιοι και $s \in S$. Τότε οι παρακάτω συνθήκες είναι ισοδύναμες*

*(i)* *το s είναι ακέραιο πάνω από το R,*

*(ii)* *ο υποδακτύλιος $R[s]$ του S είναι πεπερασμένα παραγόμενο R-πρότυπο*

*(iii)* *υπάρχει υποδακτύλιος $R'$ του $S$ έτσι ώστε $R[s] \subseteq R'$ και το $R'$ είναι πεπερασμένα παραγόμενο R-πρότυπο*

*(iv)* *υπάρχει πιστό $R[s]$-πρότυπο που είναι πεπερασμένα παραγόμενο R-πρότυπο.*

**Απόδειξη.** (i) $\Rightarrow$ (ii). Από την υπόθεση έχουμε

$$s^n + r_{n-1}s^{n-1} + \cdots + r_0 = 0$$

για κάποια $r_i \in R$. Συνεπώς $s^n = -r_{n-1}s^{n-1} - \cdots - r_0$ και για κάθε $k \geq 0$ παίρνουμε

$$s^{n+k} = -r_{n-1}s^{n+k-1} - \cdots - s^k r_0.$$

Τώρα μια προφανής επαγωγή στο $k$ δείχνει ότι κάθε $s^{n+k}$ γράφεται ως $R$-γραμμικός συνδυασμός των στοιχείων

$$1 = s^0, s, s^2, \dots, s^{n-1}.$$

(ii) $\Rightarrow$ (iii). Προφανές ($R' = R[s]$).

(iii) $\Rightarrow$ (iv). Έστω $M = R'$. Αυτό είναι πιστό $R[s]$-πρότυπο, γιατί αν $a \in \operatorname{Ann}_{R[s]} R'$, τότε $a = a1_R = 0$.

(iv) $\Rightarrow$ (i). Έστω $M$ πιστό $R[s]$-πρότυπο που είναι πεπερασμένο παραγόμενο ως $R$-πρότυπο. Εφαρμόζουμε την Πρόταση 7.1.1 για $I = R$, $S = R[s]$ και συμπεραίνουμε ότι υπάρχουν $r_1,\dots,r_{n-1} \in R$ με την ιδιότητα

$$s^n + r_{n-1}s^{n-1} + \cdots + r_0 \in \operatorname{Ann}_{R[s]} M.$$

Αλλά $\mathrm{Ann}_{R[s]}M = 0$. □

**7.2.3 Πόρισμα** *Έστω δακτύλιοι* $R \subseteq S$ *και στοιχεία* $s_1,...,s_n \in S$ *ακέραια πάνω από το R. Τότε ο δακτύλιος* $R[s_1,...,s_n]$ *είναι πεπερασμένα παραγόμενο R-πρότυπο.*

**Απόδειξη.** Επαγωγή στο $n$. Η περίπτωση $n=1$ περιέχεται στην προηγούμενη πρόταση. Για $n>1$ γράφουμε

$$R[s_1,...,s_n] = R[s_1,...,s_{n-1}][s_n].$$

Από την υπόθεση της επαγωγής το $R[s_1,...,s_{n-1}]$ είναι πεπερασμένα παραγόμενο $R$-πρότυπο. Το $R[s_1,...,s_{n-1}][s]$ είναι πεπερασμένο παραγόμενο $R[s_1,...,s_{n-1}]$ (αφού είναι ακέραιο πάνω από το $R \subseteq R[s_1,...,s_{n-1}]$). Από το Λήμμα 7.2.1, το $R[s_1,...,s_{n-1}][s_n]$ είναι πεπερασμένο παραγόμενο $R$-πρότυπο. □

**7.2.4 Ορισμός** *Έστω* $R \subseteq S$ *δακτύλιοι. Το σύνολο*

$$R' = \{s \in S \mid s \text{ είναι ακέραιο πάνω από το } R\}$$

*ονομάζεται ακέραια θήκη του* $R$ *στο* $S$. *Αν* $R' = R$, *το* $R$ *ονομάζεται ακέραια κλειστό στο* $S$.

**7.2.5 Πόρισμα** *Έστω δακτύλιοι* $R \subseteq S$. *Η ακέραια θήκη του* $R$ *στο* $S$ *είναι υποδακτύλιος του* $S$ *που περιέχει το* $R$.

**Απόδειξη.** Προφανώς $R \subseteq R'$. Έστω $a,b \in R'$. Ο δακτύλιος $R[a,b]$ είναι πεπερασμένα παραγόμενο $R$-πρότυπο (Πόρισμα 7.2.3). Από την Πρόταση 7.2.2.(iii) συμπεραίνουμε τότε ότι $a-b \in R'$ και $ab \in R'$. Άρα το $R'$ είναι δακτύλιος. □

Το προηγούμενο πόρισμα δεν αποδεικνύεται εύκολα με χρήση μόνο του ορισμού ακεραίου στοιχείου. Δοκιμάστε για παράδειγμα να βρείτε ένα μονικό πολυώνυμο στο $R[x]$ με ρίζα το $\alpha+\beta$, όπου $\alpha$, $\beta$ είναι ακέραια πάνω από το $R$. Εδώ φαίνεται η ισχύς των γενικών μεθόδων και ειδικότερα της Πρότασης 7.2.2.

**7.2.6 Πόρισμα** *Έστω $R \subseteq S \subseteq T$ δακτύλιοι με $S$ ακέραιο πάνω από το $R$ και $T$ ακέραια πάνω από το $S$. Τότε το $T$ είναι ακέραιο πάνω από το $R$.*

**Απόδειξη.** Έστω $t \in T$. Το $t$ είναι ακέραιο πάνω από το $S$. Άρα

$$t^m + s_{m-1}t^{m-1} + \cdots + s_0 = 0$$

για κάποια $s_{m-1},...,s_0 \in S$. Άρα το $t$ είναι ακέραιο πάνω από το $R[s_0,...,s_{m-1}]$. Από την Πρόταση 7.2.2, το $R[s_0,...,s_{m-1}][t]$ είναι πεπερασμένα παραγόμενο $R[s_0,...,s_{m-1}]$-πρότυπο. Το $R[s_0,...,s_{m-1}][t]$ είναι τότε πεπερασμένα παραγόμενο $R$-πρότυπο γιατί το $R[s_0,...,s_{m-1}]$ είναι πεπερασμένα παραγόμενο $R$-πρότυπο (Πόρισμα 7.2.3) οπότε εφαρμόζει το Λήμμα 7.2.1. Από την Πρόταση 7.2.2, το $t$ είναι ακέραιο πάνω από το $R$. Συνεπώς το $T$ είναι ακέραιο πάνω από το $R$. □

**7.2.7 Πόρισμα** *Έστω $R \subseteq S$. Έστω $R'$ η ακέραια θήκη του R στο S. Τότε το $R'$ είναι ακέραια κλειστό στο S.*

**Απόδειξη.** Έστω $R''$ η ακέραια θήκη του $R'$ στο $S$. Από το Πόρισμα 7.2.6, το $R''$ είναι ακέραιο πάνω από το $R$. Συνεπώς $R'' \subseteq R'$ και άρα $R' = R''$. □

## 7.3 Κανονικοποίηση της Noether

Είμαστε σε θέση να αποδείξουμε τώρα το κύριο αποτέλεσμα αυτού του κεφαλαίου.

Έστω $k$ ένα σώμα. Υπενθυμίζουμε ότι κάθε πεπερασμένα παραγόμενη $k$-άλγεβρα έχει τη μορφή $k[a_1,...,a_m]$ για κάποια $a_1,...,a_m$. Στοιχεία $y_1,...,y_n \in k[a_1,...,a_m]$ λέγονται *αλγεβρικά ανεξάρτητα* πάνω από το $k$ αν δεν υπάρχει μη μηδενικό πολυώνυμο $f(x_1,...,x_n) \in k[x_1,...,x_n]$ με την ιδιότητα $f(y_1,...,y_n) = 0$. Ισοδύναμα τα $y_1,...,y_n$ είναι αλγεβρικά ανεξάρτητα αν ο επιμορφισμός δακτυλίων

$$k[x_1,...,x_n] \ni f(x_1,...,x_n) \mapsto f(y_1,...,y_n) \in k[y_1,...,y_n]$$

είναι ισομορφισμός.

**7.3.1 Θεώρημα** *(Λήμμα Κανονικοποίησης της Noether). Έστω* $k$ *ένα άπειρο σώμα και* $R$ *μια πεπερασμένη παραγόμενη* $k$ *άλγεβρα. Τότε υπάρχουν* $z_1,...,z_m \in R$, *όπου* $m \geq 0$, *με τις ιδιότητες*

*(i)* *τα* $z_1,...,z_m$ *είναι αλγεβρικά ανεξάρτητα πάνω από το* $k$

*(ii)* *το* $R$ *είναι πεπερασμένα παραγόμενο* $S$*-πρότυπο, όπου* $S = k[z_1,...,z_m]$.

Πρώτα, μια χρήσιμη παρατήρηση. Έστω $f(x_1,...,x_n) \in k[x_1,...,x_n]$ ένα μη μηδενικό πολυώνυμο. Τότε, αν το $k$ είναι άπειρο σώμα υπάρχουν $b_1,...,b_n \in k$ με την ιδιότητα $f(b_1,...,b_n) \neq 0$. Απόδειξη: επαγωγή στο $n$. Για $n=1$, το ζητούμενο προκύπτει από το γεγονός ότι κάθε πολυώνυμο μιας μεταβλητής $f(x) \in k[x]$ ($f(x) \neq 0$) έχει το πολύ $\deg f(x)$ ρίζες στο $k$. Έστω $n>1$ και υποθέτουμε ότι στο $f(x_1,...,x_n)$ εμφανίζεται με μη μηδενικό συντελεστή η μεταβλητή $x_n$. Θεωρώντας $f(x_1,...,x_n) \in k[x_1,...,x_{n-1}][x_n]$ γράφουμε $f(x_1,...,x_n) = f^{(m)}(x_1,...,x_{n-1})\ x_n^m + \cdots + f^{(1)}(x_1,...,x_{n-1})x + f^{(0)}(x_1,...,x_{n-1})$ με $f^{(i)}(x_1,...,x_{n-1}) \in k[x_1,...,x_{n-1}]$. Από την υπόθεση της επαγωγής υπάρχουν $b_1,...,b_{n-1} \in k$ έτσι ώστε το $f(b_1,...,b_{n-1},x_n) \in k[x_n]$ είναι μη μηδενικό. Από την περίπτωση $n=1$, μπορούμε να επιλέξουμε $b_n \in k$ με την ιδιότητα $f(b_1,...,b_{n-1},b_n) \neq 0$.

**Απόδειξη του Θεωρήματος 7.3.1**

*Ισχυρισμός:* έστω $f(x_1,...,x_n) \in k[x_1,...,x_n]$ με $f(x_1,...,x_n) \neq 0$. Τότε υπάρχουν $b_1,...,b_{n-1} \in k$ με την ιδιότητα ο μεγιστοβάθμιος συντελεστής του $x_n$ του πολυωνύμου

$$f(x_1' + b_1 x_n,..., x_{n-1}' + b_{n-1}x_n) \in k[x_1',...,x_{n-1}',x_n]$$

είναι ένα μη μηδενικό στοιχείο του $k$.

*Απόδειξη.* Έστω $d = \deg f(x_1,...,x_n)$ και γράφουμε

$$f = f_d + g$$

όπου το $f_d$ είναι ομογενές πολυώνυμο βαθμού $d$ και $\deg g \leq d-1$. Έχουμε

$$f(x_1' + b_1 x_n,..., x_{n-1}' + b_{n-1}x_n, x_n) = f_d(b_1,...,b_{n-1},1)x_n^d + \cdots,$$

όπου $\cdots$ σημαίνει άθροισμα όρων που έχουν βαθμό ως προς $x_n$ μικρότερο από $d$. Από την παρατήρηση που διατυπώσαμε αμέσως μετά το Θεώρημα 7.3.1, συμπεραίνουμε ότι $f_d(b_1,...,b_{n-1},1) \neq 0$ για κάποια $b_1,...,b_{n-1} \in k$.

Ερχόμαστε τώρα στην απόδειξη του Θεωρήματος. Έστω $R = k[a_1,...,a_n]$. Θεωρούμε τον επιμορφισμό δακτυλίων

$$\varphi : k[x_1,...,x_n] \ni f(x_1,...,x_n) \mapsto f(a_1,...,a_n) \in R .$$

Επαγωγή στο $n$. Έστω $n=1$. Αν $\ker\varphi = 0$, τότε το $a_1$ είναι αλγεβρικά ανεξάρτητο πάνω από το $k$ και $R = k[a_1]$ είναι πεπερασμένα παραγόμενο $k[a_1]$-πρότυπο. Αν $\ker\varphi \neq 0$, τότε το $R = k[a_1]$ είναι πεπερασμένα παραγόμενο $k$-πρότυπο λόγω της Πρότασης 7.2.2, αφού το $a$ ικανοποιεί μία σχέση $f(a)=0$, $f(x_1) \neq 0$, που μπορεί να ληφθεί ως μονική (καθώς οι συντελεστές του $f(x_1)$ είναι από σώμα). Έστω $n>1$. Αν $\ker\varphi = 0$, τότε τα $a_1,...,a_n$ είναι αλγεβρικά ανεξάρτητα πάνω από το $k$. Έστω $\ker\varphi \neq 0$ και $f \in \ker\varphi$, $f \neq 0$. Από τον ισχυρισμό υπάρχουν $b_1,...,b_{n-1} \in k$ έτσι ώστε το πολυώνυμο $f(x_1' + b_1 x_n,..., x_{n-1}' + b_{n-1}x_n, x_n)$ έχει αντιστρέψιμο μεγιστοβάθμιο συντελεστή του $x_n$. Επειδή $f(a_1,...,a_n)=0$ παίρνουμε ότι το $a_n$ είναι ακέραιο πάνω από το

$$R' = k[a_1',...,a_{n-1}'],$$

όπου $a_i' = a_i - b_i a_n$. Από την επαγωγική υπόθεση υπάρχουν $y_1,...,y_m \in R'$ με τις ιδιότητες (i) τα $y_1,...,y_m$ είναι αλγεβρικά ανεξάρτητα πάνω από το $k$, και (ii) $R'$ είναι πεπερασμένα παραγόμενο $k[y_1,...,y_m]$-πρότυπο. Τώρα από την Πρόταση 7.2.2, το $R = R'[a_n]$ είναι πεπερασμένα παραγόμενο $R'$-πρότυπο, και άρα (Λήμμα 7.2.1) το $R$ είναι πεπερασμένα παραγόμενο $k[y_1,...,y_m]$-πρότυπο. □

**Σημείωση:** 1) Το θεώρημα ισχύει και χωρίς την υπόθεση ότι το $k$ είναι άπειρο. Όμως η παραπάνω απόδειξη δεν ισχύει (Άσκηση 1). Εμείς θα αρκεστούμε στην περίπτωση που το $k$ είναι άπειρο, γιατί θα εφαρμόσουμε το θεώρημα στην απόδειξη του Nullstellensatz, όπου το σώμα είναι αλγεβρικά κλειστό (και συνεπώς άπειρο). 2) Το θεώρημα δεν μας πληροφορεί μόνο ότι κάθε πεπερασμένη $k$-άλγεβρα αποτελείται από ένα υπερβατικό τμήμα και ένα αλγεβρικό. Το αλγεβρικό

τμήμα έχει ειδικό χαρακτήρα: τα στοιχεία του $R$ είναι ρίζες *μονικών* πολυωνύμων με συντελεστές από το $k[y_1,...,y_m]$.

## 7.4 Εφαρμογή: Αναλλοίωτες Πεπερασμένων Ομάδων

Χρησιμοποιώντας ιδέες που αφορούν ακέραια εξάρτηση (§ 7.2) και δακτύλιους της Noether (Κεφάλαιο 4) θα αποδείξουμε εδώ ένα σημαντικό θεώρημα της E. Noether (1916 και 1926) για αναλλοίωτες. Το θεώρημα δίνει καταφατική απάντηση στην ειδική περίπτωση του 14ου προβλήματος του Hilbert που αφορά τη δράση *πεπερασμένης* ομάδας ως ομάδα αυτομορφισμών μιας πεπερασμένα παραγόμενης $R$-άλγεβρας, όπου $R$ δακτύλιος της Noether (δες την εισαγωγή).

Έστω λοιπόν $R$ ένας δακτύλιος της Noether και $S = R[s_1,...,s_m]$ μια πεπερασμένα παραγόμενη $R$-άλγεβρα. Έστω $G$ μια πεπερασμένη ομάδα $R$-αυτομορφισμών της $S$. Το σύνολο των αναλλοιώτων

$$S^G = \{s \in S \mid g(s) = s \text{ για κάθε } g \in G\},$$

είναι $R$-υποάλγεβρα του $S$.

**7.4.1 Θεώρημα** *(E. Noether). Με τις προηγούμενες υποθέσεις η $R$-άλγεβρα $S^G$ είναι πεπερασμένα παραγόμενη.*

Για την απόδειξη θα εφαρμόσουμε το ακόλουθο κριτήριο.

**7.4.2 Πρόταση** *Έστω δακτύλιοι $R \subseteq T \subseteq S$. Υποθέτουμε ότι*

*(i) $R$ είναι της Noether*

*(ii) $S$ είναι πεπερασμένα παραγόμενη $R$-άλγεβρα*

*(iii) $S$ είναι ακέραιο πάνω από το $T$.*

Τότε η $R$-άλγεβρα $T$ είναι πεπερασμένα παραγόμενη.

**Απόδειξη.** Πρώτα παρατηρούμε ότι το $S$ είναι πεπερασμένα παραγόμενο $T$-πρότυπο. Πράγματι, από το ii) έχουμε $S = R[s_1,...,s_m]$, $s_i \in S$. Επειδή κάθε $s_i$ είναι ακέραιο επί του $T$, ισχύει το Πόρισμα 7.2.3 οπότε το $S$ είναι πεπερασμένο παραγόμενο $T$-πρότυπο.

Έστω ότι τα $s_1',...,s_n'$ παράγουν το $S$ ως $T$-πρότυπο, δηλαδή

$$S = Ts_1' + \cdots + Ts_n' .$$

Τότε για κάποια $t_{ij}, t_{ijk} \in T$ έχουμε

$$s_i = \sum_j t_{ij} s_j' \tag{3}$$

$$s_i' s_j' = \sum_k t_{ijk} s_k' . \tag{4}$$

Έστω $T_0$ η $R$-άλγεβρα που παράγεται απ' όλα τα $t_{ij}$, $t_{ijk}$. Τότε ο $T_0$ είναι δακτύλιος της Noether (Θεώρημα Βάσης του Hilbert και Πρόταση 4.1.4). Επιπλέον $R \subseteq T_0 \subseteq T$.

Από τις (3) και (4) έπεται ότι κάθε στοιχείο του $S$ είναι γραμμικός συνδυασμός των $s_k'$ με συντελεστές από το $T_0$. Δηλαδή το $S$ είναι πεπερασμένα παραγόμενο $T_0$-πρότυπο. Αφού ο $T_0$ είναι δακτύλιος της Noether, το $S$ είναι $T_0$-πρότυπο της Noether (Πόρισμα 5.2.3(i)). Άρα και το $T$ είναι $T_0$-πρότυπο της Noether, αφού $T \subseteq S$ (Πρόταση 5.2.1(i)), και συνεπώς πεπερασμένα παραγόμενο (Πρόταση 5.1.1(iii)). Όμως το $T_0$ είναι πεπερασμένα παραγόμενη $R$-άλγεβρα (από τον ορισμό). Άρα και το $T$ είναι πεπερασμένα παραγόμενη $R$-άλγεβρα.

□

**Απόδειξη του Θεωρήματος 7.4.1**

Γράφουμε $S = R[s_1,...,s_n]$. Στον πολυωνυμικό δακτύλιο $S[t]$ θεωρούμε τα πολυώνυμα

$$p_i(t) = \prod_{g \in G} (t - g(s_i)) .$$

Επεκτείνουμε τη δράση της $G$ στο $S[t]$ κατά τον προφανή τρόπο: αν $f_m t^m + \cdots + f_0 \in S[t]$, θέτουμε $g(f_m t^m + \cdots + f_0) = g(f_m)t^m + \cdots + g(f_0)$ για κάθε $g \in G$. Έστω τώρα $h \in G$. Έχουμε

$$h(p_i(t)) = \prod_{g \in G} (t - (hg)(s_i)) = p_i(t) ,$$

γιατί το $hg$ διατρέχει τα στοιχεία της $G$ καθώς το $g$ διατρέχει τα στοιχεία της $G$. Επομένως οι συντελεστές του $p_i(t)$ ανήκουν στο $S^G$. Επειδή κάθε $p_i(t)$ είναι

μονικό και έχει ρίζα το $s_i$ συμπεραίνουμε ότι κάθε $s_i$ είναι ακέραιο πάνω από το $S^G$. Άρα ο $S = R[s_1,...,s_n]$ είναι ακέραιος πάνω από το $S^G$ (γιατί η ακέραια θήκη του $S^G$ στο $S$ είναι δακτύλιος, Πόρισμα 7.2.5).

Τέλος έχουμε

$$R \subseteq S^G \subseteq S,$$

οπότε το ζητούμενο προκύπτει αμέσως από την Πρόταση 7.4.2. □

**Σχόλιο.** Για άπειρες ομάδες $G$ το παραπάνω θεώρημα δεν ισχύει γενικά. Το πρώτο αντιπαράδειγμα βρέθηκε το 1958 από τον Nagata ο οποίος έτσι απάντησε αρνητικά στο 14ο πρόβλημα του Hilbert (δες την Εισαγωγή).

## Ασκήσεις

**1.** Δείξτε με ένα παράδειγμα ότι η απόδειξη του λήμματος κανονικοποίησης της Noether που δώσαμε δεν ισχύει γενικά για πεπερασμένα σώματα (Υπόδειξη: βρείτε ένα πολυώνυμο $f(x,y)$ για το οποίο το $f_d(x,y)$ ικανοποιεί $f_d(a,1) = a^p - a = 0$ για κάθε $a \in \mathbb{Z}_p$).

**2.** Έστω $k \subseteq S$ δακτύλιοι, όπου το $k$ είναι σώμα και το $S$ είναι πεπερασμένα παραγόμενο $k$-πρότυπο και ακέραια περιοχή. Τότε το $S$ είναι σώμα.

**3.** Έστω $R \subseteq S$ ακέραιες περιοχές έτσι ώστε κάθε $s \in S$ είναι ακέραιο πάνω από το $R$. Τότε το $R$ είναι σώμα αν και μόνο αν το $S$ είναι σώμα.

**4.** (Ασθενές Nullstellensatz). Έστω $k$ άπειρο σώμα και $K$ μια $k$-άλγεβρα που είναι

(i) πεπερασμένα παραγόμενη $k$-άλγεβρα

(ii) σώμα.

Τότε κάθε στοιχείο του $K$ είναι αλγεβρικό πάνω από το $k$.

(Υπόδειξη: εφαρμόσετε το λήμμα κανονικοποίησης της Noether και χρησιμοποιήσετε την άσκηση 3).

**5.** Έστω $n \in \mathbb{N}$ ακέραιος που δεν διαιρείται από τετράγωνο άλλου ακέραιου $\neq 1$. Θεωρούμε το σώμα $k = \mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} \mid a,b \in \mathbb{Q}\}$. Αποδείξετε ότι το

στοιχείο $a+b\sqrt{n}$ είναι ακέραιο πάνω στο *Z* αν και μόνο αν είτε $a,b\in\mathbb{Z}$ είτε $n\equiv 1 \bmod 4$ και $2(a-b)\in\mathbb{Z}$.

**6.** Έστω $R=k[x,y]/(y^2-x^3)$, όπου *k* σώμα. Είναι το *R* ακέραια περιοχή; περιγράψτε το σώμα πηλίκων του *R*. Έστω $\overline{R}$ η ακέραια θήκη του *R* στο σώμα πηλίκων του. Ισχύει $\overline{R}=R$; (Ακέραιες περιοχές *R* με την ιδιότητα $\overline{R}=R$ ονομάζονται *κανονικές*).

**7.** Κάθε περιοχή μοναδικής παραγοντοποίησης είναι κανονική. (Δες την προηγούμενη άσκηση).

**8.** Δώστε μια άλλη απόδειξη του λήμματος του Nakayama, με επαγωγή στο ελάχιστο αριθμό γεννητόρων του *M*.

**9.** Έστω *I* ένα ιδεώδες του *R* με την ιδιότητα $I^2=I$. Τότε $I=(e)$, για κάποιο $e\in I$ που ικανοποιεί $e^2=e$. (Υπόδειξη: πόρισμα 7.1.2).

**10.** Έστω *R* ένας τοπικός δακτύλιος με μέγιστο ιδεώδες $\underline{m}$ και *M* πεπερασμένα παραγόμενο *R*-πρότυπο. Γράφουμε $\overline{M}=M/\underline{m}M$ και αν $s\in M$ γράφουμε $\bar{s}$ για την εικόνα του *s* στο $\overline{M}$. Έστω $s_1,\ldots,s_n\in M$. Τότε τα $\bar{s}_1,\ldots,\bar{s}_n$ είναι βάση του $R/\underline{m}$-διανυσματικού χώρου $M/\underline{m}M$ αν και μόνο αν το σύνολο $\{s_1,\ldots,s_n\}$ είναι ένα ελάχιστο σύνολο γεννητόρων του *M*. (Υπόδειξη: ίσως ο Nakayama σας βοηθήσει).

**11.** Έστω $p\in\mathbb{Z}$ ένας πρώτος αριθμός του $\mathbb{Z}_{(p)}=\left\{\frac{a}{b}\in\mathbb{Q}\mid p \text{ δεν διαιρεί το } b\right\}$. Ο $\mathbb{Z}_{(p)}$ είναι τοπικός δακτύλιος με μέγιστο ιδεώδες το $(p)=p\mathbb{Z}_{(p)}$. Θεωρούμε το $\mathbb{Q}$ ως $\mathbb{Z}_{(p)}$-πρότυπο $(\mathbb{Z}_{(p)}\subseteq\mathbb{Q})$. Ισχύει $(p)Q=Q$ αλλά $Q\neq 0$. Έτσι το λήμμα του Nakayama *δεν* ισχύει γενικά για μη πεπερασμένα παραγόμενα πρότυπα.

# Κεφάλαιο 8

# Ομοπαραλληλικές Πολλαπλότητες και το Nullstellensatz

Στο κεφάλαιο αυτό θα ασχοληθούμε με ομοπαραλληλικές πολλαπλότητες και τη σχέση τους με πεπερασμένα παραγόμενες άλγεβρες. Θα αποδείξουμε το Nullstellensatz και θα εξετάσουμε συνοπτικά τη γέφυρα που αυτό παρέχει μεταξύ Άλγεβρας και Γεωμετρίας.

## 8.1 Ομοπαραλληλικές Πολλαπλότητες

Στο κεφάλαιο αυτό $k$ συμβολίζει ένα σώμα.

Αν $J$ είναι ιδεώδες του πολυωνυμικού δακτυλίου $k[x_1,...,x_n]$, με $V(J)$ συμβολίζουμε το υποσύνολο του $k^n = k \times \cdots \times k$ που ορίζεται από τη σχέση

$$V(J) = \{P \in k^n \mid f(P) = 0 \quad \text{για κάθε} \quad f \in J\},$$

όπου τα σημεία του $k^n$ συμβολίζονται με $P = (a_1,...,a_n)$ και $f(P) = f(a_1,...,a_n)$. Έτσι το $V(J)$ είναι το σύνολο των σημείων του $k^n$ στα οποία κάθε πολυώνυμο του $J$ μηδενίζεται.

**8.1.1 Ορισμός** *Ένα υποσύνολο $X \subseteq k^n$ ονομάζεται αλγεβρικό ή ομοπαραλληλική πολλαπλότητα αν $X = V(J)$ για κάποιο ιδεώδες $J$ του $k[x_1,...,x_n]$.*

Αν $\{f_i \mid I \in i\}$ είναι ένα σύνολο πολυωνύμων του $k[x_1,...,x_n]$ τότε το σύνολο των σημείων του $k^n$ όπου κάθε $f_i$ μηδενίζεται είναι το $V(J)$, όπου $J$ είναι το ιδεώδες του $k[x_1,...,x_n]$ που παράγεται από το $\{f_i \mid i \in I\}$. Για τον λόγο αυτό, η απαίτηση στον ορισμό το $J$ να είναι ιδεώδες δεν μας περιορίζει.

Έστω $J$ ένα ιδεώδες του $k[x_1,...,x_n]$. Επειδή ο $k[x_1,...,x_n]$ είναι δακτύλιος της Noether (Πόρισμα 4.2.2), το $J$ είναι πεπερασμένα παραγόμενο. Έστω $J=(f_1,...,f_m)$. Τότε το $P\in k^n$ ικανοποιεί το σύστημα

$$f_1(P)=f_2(P)=\cdots=f_m(P)=0$$

αν και μόνο αν

$$P\in V(J).$$

Επομένως οι ομοπαραλληλικές πολλαπλότητες είναι ακριβώς τα υποσύνολα του $k^n$ που είναι λύσεις κάποιων συστημάτων πολυωνυμικών εξισώσεων. Η μελέτη τέτοιων υποσυνόλων του $k^n$ είναι –μιλώντας με μεγάλο βαθμό ελευθερίας– το αντικείμενο της Αλγεβρικής Γεωμετρίας.

**8.1.2 Πρόταση** *Έστω ιδεώδη I, J του* $k[x_1,...,x_n]$. *Τότε έχουμε*

*(i)* $V(0)=k^n$, $V(k[x_1,...,x_n])=\varnothing$

*(ii)* $I\subseteq J\Rightarrow V(I)\supseteq V(J)$

*(iii)* $V(I\cap J)=V(I)\cup V(J)$

*(iv)* $V\left(\sum_{\lambda\in\Lambda} I_\lambda\right)=\bigcap_{\lambda\in\Lambda} V(I_\lambda)$ *για οποιαδήποτε οικογένεια* $(I_\lambda)_{\lambda\in\Lambda}$ *ιδεωδών του* $k[x_1,...,x_n]$.

**Απόδειξη.** (i) Προφανής

(ii) $V(J)=\{P\in k^n \mid f(P)=0$ για κάθε $f\in J\}\subseteq\{P\in k^n \mid f(P)=0$ για κάθε $f\in I\}$ γιατί $I\subseteq J$. Άρα $V(J)\subseteq V(I)$.

(iii) Από το (ii) προκύπτει ότι $V(I)\cup V(J)\subseteq V(I\cap J)$. Έστω τώρα $P\in V(I\cap J)$. Αν $P\notin V(I)\cup V(J)$, τότε θα υπήρχαν $f\in I$ και $g\in J$ με τις ιδιότητες $f(P)\neq 0$ και $g(P)\neq 0$. Αλλά τότε $(fg)(P)\neq 0$, που είναι άτοπο γιατί $fg\in I\cap J$ και $P\in V(I\cap J)$.

(iv) $P\in V\left(\sum_{\lambda\in\Lambda} I_\lambda\right)\Leftrightarrow f(P)=0$ για κάθε $f\in\bigcup_{\lambda\in\Lambda} I_\lambda\Leftrightarrow P\in\bigcup_{\lambda\in\Lambda} V(I_\lambda)$. □

Θεωρούμε την τοπολογία στο $k^n$ όπου τα *κλειστά* σύνολα είναι τα αλγεβρικά. Η προηγούμενη πρόταση μας πληροφορεί ότι πράγματι ορίζεται έτσι μια τοπολογία. Αυτή ονομάζεται *τοπολογία του Zariski* στο $k^n$. Αν $X$ είναι αλγεβρικό υποσύνολο του $k^n$, τότε ορίζουμε μία τοπολογία στο $X$ παίρνοντας ως κλειστά σύνολα τις τομές του $X$ με τα κλειστά σύνολα του $k^n$. Αυτή φυσικά ονομάζεται τοπολογία του Zariski στο $X$. Στις σημειώσεις αυτές δεν θα μας ενδιαφέρουν τοπολογικές ιδιότητες αλγεβρικών συνόλων, αλλά απλώς θα χρησιμοποιούμε την ορολογία και τις στοιχειώδεις έννοιες της Τοπολογίας για κομψότητα στις διατυπώσεις.

Αξίζει όμως να σημειωθεί ότι η τοπολογία του Zariski στο $\mathbb{R}^n$ είναι πολύ ασθενέστερη της συνηθισμένης μετρικής τοπολογίας. Για παράδειγμα, τα κλειστά σύνολα στην τοπολογία του Zariski στο $k^1 = k$ είναι τα πεπερασμένα σύνολα (γιατί κάθε πολυώνυμο $f(x) \in k[x]$ έχει πεπερασμένο πλήθος ριζών στο $k$).

Έχουμε ορίσει την απεικόνιση

$$V : \{J \mid J \text{ ιδεώδες του } k[x_1,...,x_n]\} \to \{X \mid X \text{ υποσύνολο του } k^n\}.$$

Ορίζουμε τώρα μια απεικόνιση στην αντίθετη κατεύθυνση.

$$I : \{X \mid X \text{ υποσύνολο του } k^n\} \to \{J \mid J \text{ ιδεώδες του } k[x_1,...,x_n]\},$$

$$I(X) = \{f \in k[x_1,...,x_n] \mid f(P) = 0 \text{ για κάθε } P \in X\}.$$

Επαληθεύεται άμεσα από τον ορισμό ότι το $I(X)$ είναι ιδεώδες του $k[x_1,...,x_n]$. Ποια είναι η σχέση των $V$ και $J$; Μία πρώτη (επιφανειακή) απάντηση δίνεται από την παρακάτω εύκολη πρόταση και μία δεύτερη (βαθιά) δίνεται από το Nullstellensatz, που θα δούμε σε λίγο.

**8.1.3 Πρόταση** *Έστω* $X, Y \subseteq k^n$ *και* $J$ *ιδεώδες του* $k[x_1,...,x_n]$. *Τότε έχουμε*

*(i)* $X \subseteq Y \Rightarrow I(X) \supseteq I(Y)$

*(ii)* $I(X \cup Y) = I(X) \cap I(Y)$

*(iii)* $X \subseteq V(IX))$ *με ισότητα αν και μόνο αν το* $X$ *είναι αλγεβρικό.*

*(iv)* $J \subseteq I(V(J))$.

**Απόδειξη.** (i) $f \in I(Y) \Rightarrow f(P) = 0$ για κάθε $P \in Y \Rightarrow f(P) = 0$ για κάθε $P \in X \Rightarrow f \in I(X)$.

(ii) Επίσης άμεσο, όπως και το (i).

(iii) $P \in X \Rightarrow f(P) = 0$ για κάθε $f \in I(X) \Rightarrow P \in V(I(X))$. Αν $X = V(I(X))$, τότε το $X$ είναι βέβαια αλγεβρικό. Αν το $X$ είναι αλγεβρικό, $X = V(J')$, τότε $I(X) \supseteq J'$ από τον ορισμό. Άρα $V(I(X)) \subseteq V(J') = X$ λόγω του (i).

(iv) Άμεσο από τους ορισμούς. □

Η σχέση $J \subseteq I(V(J))$ της προηγούμενης πρότασης παρουσιάζει ενδιαφέρον: πότε ισχύει $J \subsetneq I(V(J))$; Για παράδειγμα, έστω $k = \mathbb{R}$ και $J = (x^2 + 1)$. Τότε $V(J) = \varnothing$ και $I(V(J)) = I(\varnothing) = \mathbb{R}[x]$. Αυτό που συμβαίνει εδώ είναι ότι το πολυώνυμο $x^2 + 1$ δεν έχει "αρκετές" ρίζες στο $\mathbb{R}$, δηλαδή το $\mathbb{R}$ δεν είναι αλγεβρικά κλειστό.

Ένα δεύτερο παράδειγμα τώρα: έστω $J = (x^2)$. Τότε προφανώς $(x) \subseteq I(V(J))$ και έχουμε $(x^2) \subsetneq (x) \subseteq I(V(J))$. Αυτό που συμβαίνει εδώ είναι ότι τα πολυώνυμα $x^2$ και $x$ ορίζουν το ίδιο αλγεβρικό σύνολο. Όπως θα δούμε παρακάτω, το Nullstellensatz μας πληροφορεί ότι $I(V(J)) = \sqrt{J}$ (όταν το $k$ είναι αλγεβρικά κλειστό).

Οι απεικονίσεις $V$ και $I$ συνδέουν ιδεώδη (αλγεβρικά αντικείμενα) με ομοπαραλληλικές πολλαπλότητες (γεωμετρικά αντικείμενα). Ακολουθεί ένα απλό παράδειγμα αλληλεπίδρασης Άλγεβρας και Γεωμετρίας.

**8.1.4 Ορισμός** *Ένα αλγεβρικό σύνολο $X \subseteq k^n$ καλείται ανάγωγο αν δεν υπάρχουν αλγεβρικά σύνολα $X_1, X_2 \subseteq k^n$ με την ιδιότητα*

$$X = X_1 \cup X_2, \quad \textit{όπου} \quad X_1 \subsetneq X, X_2 \subsetneq X.$$

Για παράδειγμα, στο $k^2$ το $X = V(y - x^2)$ είναι ανάγωγο (άσκηση· ή δες την παρακάτω πρόταση) ενώ το $Y = V(xy)$ δεν είναι, αφού $Y = V(x) \cup V(y)$.

**8.1.5 Πρόταση** *Έστω $X \subseteq k^n$ αλγεβρικό σύνολο. Τότε*

*(i)* $X$ *ανάγωγο* $\Leftrightarrow I(X)$ *πρώτο ιδεώδες.*

*(ii)* $X = X_1 \cup \cdots \cup X_m$ *όπου κάθε* $X_i$ *είναι ανάγωγο και* $X_i \not\subseteq X_j$ *για* $i \neq j$.

**Απόδειξη.** (i) Έστω $X$ ανάγωγο και $I(X)$ όχι πρώτο. Τότε υπάρχουν $f, g \in k[x_1,...,x_n]$ με την ιδιότητα $fg \in I(X)$ και $f, g \notin I(X)$. Θεωρούμε τα ιδεώδη $I_1 = I(X) + (f)$, $I_2 = I(X) + (g)$ και τα αλγεβρικά σύνολα $X_1 = V(I_1)$, $X_2 = V(I_2)$. Έχουμε $X_1 \subsetneq X$ γιατί $f \notin I(X)$ και $f \in I(X_1)$. Όμοια $X_2 \subsetneq X$. Επίσης $X \subseteq X_1 \cup X_2$, γιατί αν $P \in X$, τότε $(fg)(P) = 0$ και συνεπώς $f(P) = 0$ ή $g(P) = 0$ δηλαδή $P \in X_1$ ή $P \in X_2$. Έτσι το $X$ δεν είναι ανάγωγο, άτοπο. Αντίστροφα, έστω $I(X)$ πρώτο και $X = X_1 \cup X_2$. Τότε $I(X) = I(X_1 \cup X_2) = I(X_1) \cap J(X_2)$. Από το Λήμμα 6.1.3(ii) έχουμε $I(X) = I(X_1)$ ή $I(X_2)$, οπότε $X = V(I(X)) = V(I(X_1)) = X_1$ ή $X = V(I(X)) = V(I(X_2)) = X_2$ από την Πρόταση 8.1.3(iii). Άρα το $X$ δεν είναι ανάγωγο.

(ii) *Ισχυρισμός:* κάθε μη κενό σύνολο $\Omega$ που αποτελείται από αλγεβρικά υποσύνολα του $k^n$ έχει ελάχιστο στοιχείο.

*Απόδειξη.* Αρκεί να δείξουμε ότι κάθε φθίνουσα ακολουθία

$$X_1 \supseteq X_2 \supseteq \cdots \tag{1}$$

αλγεβρικών υποσυνόλων του $k^n$ είναι τελικά σταθερή, δηλαδή υπάρχει $m$ με την ιδιότητα $X_m = X_{m+1} = \cdots$. Πράγματι, έστω $X_1 \in \Omega$. Αν το $X_1$ δεν είναι ελάχιστο, έχουμε $X_1 \supsetneq X_2 \supsetneq X_3$ για κάποιο $X_3 \in \Omega$ κ.λ.π. Η ακολουθία αυτή είναι τελικά σταθερή, $X_m = X_{m+1} = \cdots$ για κάποιο $m$. Προφανώς το $X_m$ είναι ελάχιστο στοιχείο. Θα δείξουμε τώρα ότι η (1) είναι τελικά σταθερή. Από την (1) και την Πρόταση 8.1.3 παίρνουμε

$$I(X_1) \subseteq I(X_2) \subseteq \cdots$$

που είναι μια αύξουσα ακολουθία ιδεωδών του δακτυλίου $k[x_1,...,x_n]$ που είναι της Noether (Πόρισμα 4.2.2). Συνεπώς έχουμε

$$I(X_m) = I(X_{m+1}) = \cdots$$

για κάποιο $m$. Άρα

$$V(I(X_m)) = V(I(X_{m+1})) = \cdots$$

δηλαδή $X_m = X_{m+1} = \cdots$ από την Πρόταση 7.1.3(iii). Αποδείξαμε τον ισχυρισμό.

Θα αποδείξουμε τώρα το (ii) της πρότασης. Έστω $\Omega$ το σύνολο των αλγεβρικών συνόλων $X$ που δεν γράφονται ως

$$X = X_1 \cup \cdots \cup X_m$$

για κάποιο $m$, όπου το $X_i$ είναι ανάγωγο και $X_i \not\subseteq X_j$ για $i \neq j$. Θα δείξουμε ότι $\Omega = \varnothing$. Έστω ότι $\Omega \neq \varnothing$. Από τον ισχυρισμό, το $\Omega$ έχει ελάχιστο στοιχείο, έστω $X$. Αν το $X$ είναι ανάγωγο τότε $X \notin \Omega$, άτοπο. Αν το $X$ δεν είναι ανάγωγο, τότε $X = X_1 \cup X_2$ για κάποια αλγεβρικά σύνολα με $X_1, X_2 \subsetneq X$. Από τον ορισμό του $X$ έχουμε $X_1 \notin \Omega$ και $X_2 \notin \Omega$. Όμως τότε το $X_1$ και το $X_2$ είναι ένωση αναγώγων συνόλων, οπότε και το $X = X_1 \cup X_2$ είναι ένωση αναγώγων συνόλων, πάλι άτοπο. □

Η προηγούμενη πρόταση μας πληροφορεί ότι κάθε αλγεβρικό σύνολο $X$ γράφεται ως ένωση αναγώγων συνόλων. Τα $X_i$ που εμφανίζονται είναι μοναδικά (Άσκηση 20) και ονομάζονται *ανάγωγες συνιστώσες* του $X$.

## 8.2 Nullstellensatz

Είδαμε ότι για κάθε ιδεώδες $J$ του $k[x_1,...,x_n]$ ισχύει $J \subseteq I(V(J))$. Τώρα θα αποδείξουμε κάτι σαφώς ισχυρότερο. Πρώτα υπενθυμίζουμε ότι το ριζικό του $J$ είναι $\sqrt{J} = \{ f \in k[x_1,...,x_n] \mid f^m \in J \text{ για κάποιο } m \in \mathbb{N} \}$ (§ 6.1).

**8.2.1 Θεώρημα** *(Nullstellensatz=Θεώρημα ριζών). Έστω k ένα αλγεβρικά κλειστό σώμα. Τότε ισχύουν οι εξής προτάσεις.*

*(i) Κάθε μέγιστο ιδεώδες του* $k[x_1,...,x_n]$ *είναι της μορφής*

$$(x_1 - a_1,..., x_n - a_n)$$

*για κάποιο* $(a_1,...,a_n) \in k^n$.

*(ii) Αν* $J \neq k[x_1,...,x_n]$ *είναι ιδεώδες, τότε* $V(J) \neq \varnothing$.

*(iii) Για κάθε ιδεώδες J του* $k[x_1,...,x_n]$ *ισχύει*

$$I(V(J)) = \sqrt{J}\ .$$

Το (ii) μας πληροφορεί ότι οποιαδήποτε πολυώνυμα του $k[x_1,...,x_n]$ που δεν παράγουν το $k[x_1,...,x_n]$ έχουν κοινή ρίζα. Το (iii) λέει ότι αν ένα πολυώνυμο μηδενίζεται στο σύνολο των κοινών ριζών κάποιων πολυωνύμων $g_i$, τότε κάποια δύναμη του ανήκει στο ιδεώδες που παράγουν τα $g_i$.

Για την απόδειξη χρειαζόμαστε την παρακάτω σημαντική πρόταση, το δεύτερο τμήμα της οποία έπεται από το λήμμα κανονικοποίησης της Noether.

**8.2.2 Πρόταση** *(i) Έστω $R \subseteq S$ δακτύλιοι. Αν το S είναι σώμα και επιπλέον είναι πεπερασμένα παραγόμενο R-πρότυπο, τότε το R είναι σώμα.*
*(ii) Έστω k ένα άπειρο σώμα και $S = k[a_1,...,a_n]$ μια πεπερασμένη παραγόμενη k-άλγεβρα. Αν το S είναι σώμα τότε το S είναι αλγεβρικό πάνω από το k.*

**Απόδειξη.** (i) Έστω $a \in R$, $a \neq 0$. Τότε $a^{-1} \in S$. Επειδή το $S$ είναι πεπερασμένα παραγόμενο $R$-πρότυπο λόγω της Πρότασης 7.2.2 ότι

$$a^{-n} + r_{n-1}a^{-(n-1)} + \cdots + r_1 a^{-1} + r_0 = 0,$$

για κάποια $r_i \in R$. Πολλαπλασιάζοντας με $a^{n-1}$ παίρνουμε

$$a^{-1} = -(r_{n-1} + r_{n-2}a + \cdots + r_0 a^{n-1})$$

και συνεπώς $a^{-1} \in R$. Άρα το $R$ είναι σώμα.

(ii) Εφαρμόζουμε το λήμμα κανονικοποίησης της Noether. Υπάρχουν αλγεβρικά ανεξάρτητα πάνω από το $k$ στοιχεία $z_1,...,z_m \in S$ έτσι ώστε το $S$ είναι πεπερασμένα παραγόμενα $k[z_1,...,z_m]$-πρότυπο. Από το (i) συμπεραίνουμε ότι το $k[z_1,...,z_m]$ είναι σώμα. Επειδή τα $z_1,...,z_m$ είναι αλγεβρικά ανεξάρτητα πάνω από το $k$, παίρνουμε $m = 0$. Έτσι το $S$ είναι πεπερασμένα παραγόμενο $k$-πρότυπο. Από την Πρόταση 7.2.2 κάθε $s \in S$ είναι ακέραιο πάνω από το $k$ και συνεπώς αλγεβρικό πάνω από το $k$.

□

**Απόδειξη του Nullstellensatz**

(i) Θα δείξουμε ότι κάθε ιδεώδες του $k[x_1,...,x_n]$ της μορφής $(x_1 - a_1,...,x_n - a_n)$ είναι μέγιστο. Θεωρούμε τον επιμορφισμό δακτυλίων

$$\varphi : k[x_1,...,x_n] \ni f(x_1,...,x_n) \mapsto f(a_1,...,a_n) \in k .$$

Από το $1^{ο}$ Θεώρημα Ισομορφισμών Δακτυλίων (Θεώρημα 0.8.2) και την Πρόταση 0.6.4, αρκεί να δείξουμε ότι $\ker\varphi = (x_1 - a_1,..., x_n - a_n)$. Η σχέση $(x_1 - a_1,..., x_n - a_n) \subseteq \ker\varphi$ είναι προφανής. Με επαγωγή στο $n$ θα δείξουμε τον εξής *ισχυρισμό:* Έστω $f(x_1,...,x_n) \in k[x_1,...,x_n]$ με $f(a_1,...,a_n) = 0$. Τότε υπάρχουν $g_i(x_1,...,x_n) \in k[x_1,...,x_n]$ με την ιδιότητα

$$f(x_1,...,x_n) = g_i(x_1,...,x_n)(x_1 - a_1) + \cdots + g_n(x_1,...,x_n)(x_n - a_n) .$$

*Απόδειξη.* Για $n = 1$ το ζητούμενο προκύπτει αμέσως από την ταυτότητα διαίρεσης (Άσκηση 0.17) στο $k[x]$. Έστω $n > 1$. Θεωρούμε το $f(x_1,...,x_{n-1},x_n)$ ως στοιχείο του $k[x_1,...,x_{n-1}][x_n]$. Αν ο μεγιστοβάθμιος συντελεστής ως προς $x_n$ είναι μηδέν τότε $f(x_1,...,x_n) \in k[x_1,...,x_{n-1}]$ και το ζητούμενο προκύπτει αμέσως από την επαγωγική υπόθεση. Έστω λοιπόν ότι ο μεγιστοβάθμιος συντελεστής του $x_n$ δεν είναι μηδέν. Τότε από την ταυτότητα διαίρεσης έχουμε

$$f(x_1,...,x_n) = q(x_1,...,x_n)(x_n - a_n) + r(x_1,...,x_{n-1}) \qquad (2)$$

για κάποια $q(x_1,...,x_n, \in k[x_1,...,x_n]$ και $r(x_1,...,x_{n-1}) \in k[x_1,...,x_{n-1}]$. Προφανώς $r(a_1,...,a_{n-1}) = 0$. Από την επαγωγική υπόθεση έχουμε

$$r(x_1,...,x_{n-1}) = g_1(x_1,...,x_n)(x_1 - a_1) + \cdots + g_{n-1}(x_1,...,x_{n-1})(x_{n-1} - a_{n-1}) . \qquad (3)$$

Το ζητούμενο προκύπτει από τις (2) και (3). Αποδείξαμε έτσι τον ισχυρισμό. Συνεπώς το $(x_1 - a_1,..., x_n - a_n)$ είναι μέγιστο ιδεώδες.

Έστω τώρα $M$ ένα μέγιστο ιδεώδες του $k[x_1,...,x_n]$. Θα δείξουμε ότι $M = (x_1 - a_1,..., x_n - a_n)$ για κάποια $a_i \in k$. Το πηλίκο $k[x_1,...,x_n]/M$ είναι σώμα. Θεωρούμε την απεικόνιση $\varphi : k[x_1,...,x_n] / M$ που είναι η σύνθεση

$$k \to k[x_1,...,x_n] \to k[x_1,...,x_n]/M ,$$

όπου η απεικόνιση στα αριστερά είναι ο προφανής μονομορφισμός και στα δεξιά είναι ο φυσικός επιμορφισμός. Ισχύει $\varphi \neq 0$, και αφού ο $\varphi$ είναι ομομορφισμός σωμάτων θα είναι μονομορφισμός. Όμως το $k[x_1,...,x_n]/M$ είναι αλγεβρικό πάνω από το *k*. Επειδή το $k$ είναι αλγεβρικά κλειστό, συμπεραίνουμε ότι ο μονομορφισμός $\varphi$ είναι ισομορφισμός. Τώρα, έστω $a_i = \varphi^{-1}(x_i + M) \in k$, $i = 1,...,n$. Τότε για κάθε *I* έχουμε

$$x_i - a_i \in \ker(k[x_1,...,x_n] \to k[x_1,...,x_n]/M) = M \ .$$

Συνεπώς

$$(x_i - a_1,...,x_n - a_n) \subseteq M \ .$$

Επειδή το $(x_1 - a_1,...,x_n - a_n)$ είναι μέγιστο ιδεώδες (όπως είδαμε στην αρχή της απόδειξης) έχουμε $(x_1 - a_1,...,x_n - a_n) = M$ .

(ii) Αφού $J \neq k[x_1,...,x_n]$ υπάρχει μέγιστο ιδεώδες $M$ που περιέχει το $J$ (Πόρισμα 3.5.3). Από το (i), το $M$ είναι της μορφής $(x_1 - a_1,...,x_n - a_n)$. Άρα $V(M) \ni (a_1,...,a_n)$. Όμως $V(M) \subseteq V(J)$ (Πρόταση 8.1.2(iii), και άρα $V(J) \neq \varnothing$.

(iii) (Τέχνασμα του Rabinowitch). Η σχέση $\sqrt{J} \subseteq I(V(J))$ είναι εύκολη: αν $f = f(x_1,...,x_n) \in k[x_1,...,x_n]$ με $f^n \in J$ τότε $f^n(P) = 0$ για κάθε $P \in V(J)$. Άρα $f(P) = 0$ για κάθε $P \in V(J)$, δηλαδή $f \in I(V(J))$.

Για την άλλη σχέση θα εφαρμόσουμε ένα κομψό τέχνασμα. Θεωρούμε $f \in I(V(J))$ με $f \neq 0$. Έστω $y$ μια νέα μεταβλητή και $S = k[x_1,...,x_n,y]$. Στο $S$ θεωρούμε το ιδεώδες

$$J' = JS + (yf - 1)S \ .$$

*Ισχυρισμός:* $J' = S$ . Αν ήταν $J' \neq S$ τότε από το (ii) θα είχαμε

$$g(c_1,...,c_n,c_{n+1}) = 0$$

για κάποια $c_i \in k$ και για κάθε $g \in J'$. Ειδικότερα, θα είχαμε

$$f(c_1,...,c_n) = 0 \tag{4}$$

γιατί $(c_1,...,c_n,c_{n+1}) \in V(J') \Rightarrow (c_1,...,c_n) \in V(J)$, και

$$c_{n+1} f(c_1,...,c_n) - 1 = 0 \ . \tag{5}$$

Όμως οι (4) και (5) δίνουν $-1 = 0$. Άρα $J' = S$ .

Από τον ισχυρισμό παίρνουμε

$$1 = s_1 f_1 + \cdots + s_m f_m + s_0(yf - 1) \in k[x_1,...,x_n,y] \tag{6}$$

για κάποια $s_i \in S$ και $f_i \in J$. Πολλαπλασιάζοντας την (6) με $f^N$ για αρκετά μεγάλο $N$ παίρνουμε μια σχέση της μορφής

$$f^N = s_1'(x_1,...,x_n, fy) f_1 + \cdots + s_m'(x_1,...,x_n, fy) f_m + s_0'(x_1,...,x_n, fy)(yf - 1) \tag{7}$$

όπου κάθε $s_i' = f^N s_i$ είναι γραμμένο ως πολυώνυμο των $x_1,...,x_n, fy$. Η (7) είναι ταυτότητα πολυωνύμων και επομένως μπορούμε να θέσουμε $fy = 1$. Τότε βέβαια η (7) δείχνει ότι $f^N \in J$. □

Ακολουθούν μερικές άμεσες συνέπειες του Nullstellensatz. Υπενθυμίζουμε ότι είχαμε απεικονίσεις

$$\{J \mid J \text{ ιδεώδες του } k[x_1,...,x_n]\} \xrightarrow{V} \{X \mid X \subseteq k^n\}$$

$$\{X \mid X \subseteq k^n\} \xrightarrow{I} \{J \mid J \text{ ιδεώδες του } k[x_1,...,x_n]\}.$$

Ένα ιδεώδες $J$ λέγεται *ριζικό* αν $\sqrt{J} = J$. Η παραπάνω αντιστοιχίες δεν είναι γενικά $1-1$. Για παράδειγμα $V(x_1) = V(x_1^2)$. Όμως, αν περιορισθούν σε κατάλληλα υποσύνολα, τότε το Nullstellensatz μας πληροφορεί ότι αυτές είναι $1-1$. Ακριβέστερα έχουμε:

**8.2.2 Πόρισμα** *Έστω k ένα αλγεβρικά κλειστό σώμα. Τότε οι αντιστοιχίες*

$$\{J \mid J \text{ ιδεώδες του } k[x_1,...,x_n]\} \xrightarrow{V} \{X \mid X \subseteq k^n \text{ αλγεβρικό}\}$$

$$\{X \mid X \subseteq k^n \text{ αλγεβρικό}\} \xrightarrow{I} \{J \mid J \text{ ριζικό ιδεώδες του } k[x_1,...,x_n]\}$$

*είναι* $1-1$.

**Απόδειξη.** Αν $\sqrt{J} = J$ τότε $I(V(J)) = \sqrt{J} = J$ από το Nullstellensatz. Επίσης, αν $X \subseteq k^n$ είναι αλγεβρικό, τότε $V(I(X)) = X$ (Πρόταση 8.1.3). □

**8.2.3 Πόρισμα** *Έστω k αλγεβρικά κλειστό σώμα. Τότε οι αντιστοιχίες*

$$\{P \mid P \text{ πρώτο ιδεώδες του } k[x_1,...,x_n]\} \xrightarrow{V} \{X \mid X \subseteq k^n \text{ ανάγωγο}\}$$

$$\{X \mid X \subseteq k^n \text{ ανάγωγο}\} \xrightarrow{I} \{P \mid P \text{ πρώτο ιδεώδες του } k[x_1,...,x_n]\}$$

*είναι* $1-1$.

**Απόδειξη.** Έστω $P$ ένα πρώτο ιδεώδες. Ισχύει βέβαια $\sqrt{P} = P$ και άρα $I(V(P)) = \sqrt{P} = P$ από το Nullstellensatz. Το $V(P)$ είναι ανάγωγο γιατί $I(V(P)) = P$ είναι πρώτο ιδεώδες (Πρόταση 8.1.5). Επίσης αν $X \subseteq k^n$ είναι

ανάγωγο, τότε το $I(X)$ είναι πρώτο (Πρόταση 8.1.5). Βέβαια $V(I(X)) = X$ (Πρόταση 8.1.3). □

Υπενθυμίζουμε (Πρόταση 6.1.2) ότι για κάθε ιδεώδες $J$ ενός δακτυλίου $R$ ισχύει

$$\sqrt{J} = \bigcap_{\substack{P \supseteq I \\ P \text{ πρώτο}}} P .$$

Συνεπώς κάθε ριζικό ιδεώδες του $R$ είναι τομή πρώτων ιδεωδών. Το Nullstellensatz μας πληροφορεί ότι κάθε ριζικό ιδεώδες του $k[x_1,...,x_n]$ είναι τομή *πεπερασμένου* πλήθους πρώτων ιδεωδών.

**8.2.4 Πόρισμα** *Έστω $k$ αλγεβρικά κλειστό σώμα και $J$ ένα ριζικό ιδεώδες του $k[x_1,...,x_n]$. Τότε το $J$ είναι τομή πεπερασμένου πλήθους πρώτων ιδεωδών.*

**Απόδειξη.** Εφαρμόζουμε την Πρόταση 8.1.5 στο αλγεβρικό σύνολο $V(J)$

$$V(J) = X_1 \cup \cdots \cup X_m$$

όπου τα $X_i$ είναι ανάγωγα. Άρα

$$I(V(J)) = I(X_1) \cap \cdots \cap I(X_m)$$

από την Πρόταση 8.1.6. Κάθε $I(X)$ είναι πρώτο ιδεώδες από την Πρόταση 8.1.5. Από το γεγονός ότι το $J$ είναι ριζικό ιδεώδες και το Nullstellensatz, έχουμε $J = \sqrt{J} = I(V(J)) = I(X_i) \cap \cdots \cap I(X_m)$. □

Στο Κεφάλαιο 11 θα δούμε γενικότερα ότι το προηγούμενο πόρισμα ισχύει για τυχαίους δακτυλίους της Noether στη θέση του $k[x_1,...,x_n]$ (Άσκηση 8.13).

**8.2.5 Παράδειγμα** Έστω $k$ άπειρο σώμα. Στο $k[x,y,z]$ θεωρούμε το ιδεώδες $J = (xy + yz + xz, xyz)$. Θα βρούμε τις ανάγωγες συνιστώσες του $V(J)$, και όταν το $k$ είναι αλγεβρικά κλειστό θα εκφράσουμε το $\sqrt{J}$ ως τομή πρώτων ιδεωδών.

Αν $P = (a,b,c) \in V(J)$ τότε $abc = 0$ και $ab + bc + ac = 0$. Έτσι βρίσκουμε $a = b = 0$ ή $b = c = 0$ ή $a = c = 0$. Συνεπώς

$$V(J) = V(x,y) \cup V(y,z) \cup V(x,z), \qquad (8)$$

δηλαδή το $V(J)$ είναι η ένωση των τριών αξόνων.

Επειδή το $k$ είναι άπειρο, οι άξονες αυτοί είναι ανάγωγα σύνολα γιατί τα κλειστά υποσύνολα του $k$ είναι τα πεπερασμένα.

Έστω τώρα ότι το $k$ είναι αλγεβρικά κλειστό. Εφαρμόζοντας στην (8) την απεικόνιση $I$ και χρησιμοποιώντας την Πρόταση 8.1.3(ii) παίρνουμε

$$I(V(J)) = I(V(x,y)) \cap I(V(y,z)) \cap I(V(x,z)) .$$

Εφαρμόζοντας το Nullstellensatz παίρνουμε

$$\sqrt{J} = \sqrt{(x,y)} \cap \sqrt{(y,z)} \cap \sqrt{(x,z)} .$$

Τα ιδεώδη $(x,y)$, $(y,z)$, $(x,z)$ είναι πρώτα. Πράγματι, για το $(x,y)$ έχουμε $k[x,y,z]/(x,y) \cong k[z]$ που είναι ακέραια περιοχή. Όμοια και για τα άλλα δύο. Όμως κάθε πρώτο ιδεώδες είναι ριζικό. Έτσι έχουμε

$$\sqrt{J} = (x,y) \cap (y,z) \cap (x,z) .$$

**8.2.6 Παράδειγμα** Έστω $k$ ένα άπειρο σώμα. Θα προσδιορίσουμε τις ανάγωγες συνιστώσες του $V(J)$, όπου $J = (x^3 - yz, y^2 - xz)$.

Αρχικά παρατηρούμε ότι το $J$ δεν είναι πρώτο. Πράγματι,

$$x(x^2y - z^2) = y(x^3 - yz) + z(y^2 - xz) \in J . \qquad (9)$$

Αν $x \in J$, τότε $x = f(x,y,z)(x^3 - yz) + g(x,y,z)(y^2 - xz)$ για κάποια $f(x,y,z)$, $g(x,y,z) \in k[x,y,z]$. Θέτοντας $y = z = 0$ παίρνουμε $x = f(x,0,0)x^3$ που είναι άτοπο. Άρα $x \notin J$. Όμοια $x^2y - z^2 \notin J$.

Η (9) δείχνει ότι

$$V(J) = V(J,x) \cup V(J, x^2y - z^2) .$$

Τώρα $V(J,x) = V(yz, y^2, x) = V(x,y)$. Το $V(J,x)$ είναι ο άξονας των $z$, και όπως είδαμε στο προηγούμενο παράδειγμα είναι ανάγωγο. Θα αποδείξουμε τώρα ότι το $V(J, x^2y - z^2)$ είναι ανάγωγο.

Θεωρούμε την απεικόνιση

$$\varphi : k \to k^3$$
$$t \mapsto (t^3, t^4, t^5) .$$

Εύκολα επαληθεύουμε ότι $(t^3,t^4,t^5)\in V(J,x^2y-z^2)$. Άρα $\mathrm{Im}\varphi\subseteq V(J,x^2y-z^2)$. Ισχύει $\mathrm{Im}\varphi=V(J,x^2y-z^2)$. Πράγματι, αν $P=(a,b,c)\in V(J,x^2y-z^2)$ παρατηρούμε ότι: i) αν $a=0$, τότε $a=b=c=0$ και προφανώς $P\in V(J,x^2y-z^2)$, ii) αν $a\neq 0$, τότε θέτοντας $t=b/a$ εύκολα επαληθεύουμε ότι $a=t^3$, $b=t^4$ και $c=t^5$ χρησιμοποιώντας τις σχέσεις

$$a=\frac{b}{a}\frac{c}{a},\quad \frac{c}{a}=\left(\frac{b}{a}\right)^2,\quad b=\left(\frac{c}{a}\right)^2.$$

Έστω τώρα

$$C=V(J,x^2y-z^2)=X_1\cup X_2$$

με $X_1$, $X_2$ γνήσια αλγεβρικά υποσύνολα του $V(J,x^2y-z^2)$. Τότε

$$I(C)=I(X_1)\cap I(X_2). \tag{10}$$

Αν $f_1(x,y,z)\in I(X_1)$ και $f_2(x,y,z)\in I(X_2)$ τότε από την (10) έχουμε

$$f_1(x,y,z)\ f_2(x,y,z)\in I(C).$$

Άρα $f_1(P)f_2(P)=0\ \ \forall\ P\in C$. Δηλαδή $f_i(P)=0\ \ \forall\ P\in C$ για κάποιο $i$. Συνεπώς

$$f_i(t^3,t^4,t^5)=0$$

για κάθε $t\in k$. Επειδή όμως το πολυώνυμο $f_i(t^3,t^4,t^5)$ έχει πεπερασμένο πλήθος ριζών και επειδή το $k$ είναι άπειρο, συμπεραίνουμε ότι $f_i\in I(C)$. Άρα $I(X_i)\subseteq I(C)$ (Πρόταση 8.1.3) και συνεπώς $X_i\supseteq C$ (Πρόταση 8.1.3(iii)), δηλαδή $X_i=C$, που είναι άτοπο.

Η διατύπωση του επόμενου κομψού πορίσματος είναι εντελώς στοιχειώδης πράγμα που το καθιστά ιδιαίτερα ελκυστικό.

**8.2.7 Πόρισμα** *Έστω* $f_1,\dots,f_m\in k[x_1,\dots,x_n]$, *όπου το* $k$ *είναι αλγεβρικά κλειστό. Τότε το σύστημα* $f_1=f_2=\cdots=f_m=0$ *δεν έχει λύση αν και μόνο αν υπάρχουν* $g_1,\dots,g_m\in k[x_1,\dots,x_n]$ *τέτοια ώστε*

$$1=g_1f_1+\cdots+g_mf_m. \tag{11}$$

**Απόδειξη.** Το ότι η (11) συνεπάγεται τη μη ύπαρξη λύσης του συστήματος $f_1=\cdots=f_m=0$ είναι προφανές. Το αντίστροφο έπεται αμέσως από το

Nullstellensatz: $V=(f_1,...,f_m)=\varnothing \Rightarrow (f_1,...,f_m)=k[x_1,...,x_n]$. Συνεπώς υπάρχουν $g_i \in k[x_1,...,x_n]$ με $g_1 f_1 + \cdots + g_m f_m = 1$. □

## 8.3 Απεικονίσεις Ομοπαραλληλικών Πολλαπλοτήτων

Έστω $X \subseteq k^n$ ένα αλγεβρικό σύνολο και $f = f(x_1,...,x_n) \in k[x_1,...,x_n]$. Το πολυώνυμο $f$ ορίζει μια *πολυωνυμική συνάρτηση* στο $X$, που συμβολίζουμε (προσωρινά) με $\bar{f}$, κατά τον ακόλουθο τρόπο

$$\bar{f} : X \ni P \mapsto f(P) \in k .$$

Το άθροισμα και το γινόμενο δύο πολυωνυμικών συναρτήσεων στο $X$ ορίζεται με τον προφανή τρόπο: $(\bar{f}+\bar{g})(P)=\bar{f}(P)+\bar{g}(P)$ και $(\bar{f}\bar{g})(P)=\bar{f}(P)\bar{g}(P)$. Το σύνολο των πολυωνυμικών συναρτήσεων στο $X$ καθίσταται έτσι μεταθετικός δακτύλιος. Ο δακτύλιος αυτός συμβολίζεται με $k[X]$ και ονομάζεται *δακτύλιος συντεταγμένων* του $X$. Ο πυρήνας του επιμορφισμού δακτυλίων

$$k[x_1,...,x_n] \ni f \to \bar{f} \in k[X]$$

είναι $\{f \mid f(P)=0 \text{ για κάθε } P \in X\} = I(X)$. Συνεπώς (Θεώρημα 0.3.4)

$$k[x_1,...,x_n]/I(X) \cong k[X] .$$

Θα χρησιμοποιούμε την παραπάνω ταύτιση του δακτυλίου συντεταγμένων του $X$ χωρίς ιδιαίτερη μνεία.

Αν $X = V(J)$, όπου το $J$ είναι ιδεώδες του $k[x_1,...,x_n]$ τότε, υποθέτοντας ότι το $k$ είναι αλγεβρικά κλειστό, το Nullstellensatz δίνει σε συνδυασμό με τον παραπάνω ισομορφισμό ότι:

$$k[X] \cong k[x_1,...,x_n]/\sqrt{J} .$$

Ο δακτύλιος συντεταγμένων $k[X]$ είναι μια $k$-άλγεβρα κατά τον προφανή τρόπο και μάλιστα οι παραπάνω ισομορφισμοί είναι ισομορφισμοί $k$-αλγεβρών.

Έστω $X$ αλγεβρικό σύνολο. Ορίζουμε απεικονίσεις

$$V_X : \{J \mid J \text{ ιδεώδες του } k[X]\} \to \{Z \mid Z \subseteq X\}$$

$$I_X : \{Z \mid Z \subseteq X\} \to \{J \mid J \text{ ιδεώδες του } k[X]\},$$

όπου

$$V_X(J) = \{P \in X \mid f(P) = 0 \text{ για κάθε } f \in J\}$$

$$I_X(Z) = \{f \in k[X] \mid f(P) = 0 \text{ για κάθε } P \in X\}.$$

Οι απεικονίσεις $V_X$, $I_X$ έχουν παρόμοιες ιδιότητες με αυτές των απεικονίσεων $V$ και $I$ που ορίσαμε στην Παράγραφο 8.1. Θα αποδείξουμε εδώ μια μορφή του Nullstellensatz που θα βρει εφαρμογή παρακάτω (Θεώρημα 8.3.7).

**8.3.1 Πρόταση** *(Σχετικό Nullstellensatz). Έστω $k$ ένα αλγεβρικά κλειστό σώμα και $X \subseteq k^n$ αλγεβρικό σύνολο. Αν $J$ είναι ένα γνήσιο ιδεώδες του $k[X]$, τότε $V_X(J) \neq \varnothing$.*

**Απόδειξη.** Κάθε ιδεώδες $J$ του $k[X] = k[x_1,...,x_n]/I(X)$ έχει τη μορφή $\bar{J}/I(X)$ όπου $\bar{J}$ είναι γνήσιο ιδεώδες του $k[x_1,...,x_n]$ που περιέχει το $I(X)$ (Πρόταση 0.3.3). Έστω $J$ ένα γνήσιο ιδεώδες. Τότε βέβαια και το $\bar{J}$ είναι γνήσιο. Από το Nullstellensatz, $V(\bar{J}) \neq \varnothing$. Όμως από τους ορισμούς των $V(\bar{J})$ και $V_X(J)$ και το γεγονός ότι $J = \bar{J}/I(X)$ έπεται αμέσως ότι

$$V(\bar{J}) \cap X \subseteq V_X(J).$$

Αλλά $I(X) \subseteq \bar{J} \subseteq V(I(X)) = X$ (Πρόταση 8.1.2(ii) και 8.1.3(iii)). Συνεπώς $V(\bar{J}) \subseteq V_X(J)$ και άρα $V_X(J) \neq \varnothing$. □

Θα ορίσουμε τώρα την έννοια της πολυωνυμικής *απεικόνισης* μεταξύ ομοπαραλληλικών πολλαπλοτήτων. Υπογραμμίσαμε τη λέξη "απεικόνιση" γιατί *δεν θα είναι ταυτόσημες* για μας οι έννοιες πολυωνυμική συνάρτηση και πολυωνυμική απεικόνιση.

**8.3.1 Ορισμός** *Έστω $X \subseteq k^n$ και $Y \subseteq k^m$ αλγεβρικά σύνολα. Μία απεικόνιση $f: X \to Y$ ονομάζεται πολυωνυμική απεικόνιση αν υπάρχουν πολυώνυμα $f_1,..., f_m \in k[x_1,...,x_n]$ με την ιδιότητα*

$$f(P) = (f_1(P),..., f_m(P)) \in k^m$$

*για κάθε $P \in k^n$. Θα γράφουμε τότε $f = (f_1,..., f_m)$.*

Επομένως κάθε πολυωνυμική συνάρτηση $X \to k$ είναι πολυωνυμική απεικόνιση. Έστω, για παράδειγμα $y = (x^3 - y) \subseteq k^2$. Η απεικόνιση $k \ni t \mapsto (t, t^3) \in Y$ είναι πολυωνυμική, όπως είναι και η απεικόνιση $k \ni t \mapsto (t-1, (t-1)^3) \in Y$.

**8.3.2 Ορισμός** *Έστω $X \subseteq k^n$ και $Y \subseteq k^m$ αλγεβρικά σύνολα. Μια πολυωνυμική απεικόνιση $f : X \to Y$ λέγεται ισομορφισμός αν υπάρχει πολυωνυμική απεικόνιση $g : Y \to X$ με τις ιδιότητες $f \circ g = 1_Y$ και $g \circ f = 1_X$.*

Για παράδειγμα η $f : t \mapsto (t, t^3) \in Y$ που είδαμε πιο πάνω είναι ισομορφισμός γιατί η $g : Y \ni (t, t^3) \to t$ είναι πολυωνυμική και ισχύει $f(g(t, t^3)) = (t, t^3)$ και $g(f(t)) = t$ για κάθε $t \in k$.

Η σύνθεση πολυωνυμικών απεικονίσεων είναι πάλι πολυωνυμική. Πράγματι έστω $X \subseteq k^n$, $Y \subseteq k^m$, $Z \subseteq k^l$ αλγεβρικά σύνολα και $f = (f_1, ..., f_m) : X \to Y$, $g = (g_1, ..., g_l) : Y \to Z$ πολυωνυμικές απεικονίσεις.
Τότε $g \circ f = (g_1(f_1, ..., f_m), ..., g_l(f_1, ..., f_m)) : X \to Z$.

**8.3.3 Λήμμα** *Έστω X, Y δύο αλγεβρικά σύνολα. Αν η $f : X \to Y$ είναι πολυωνυμική απεικόνιση, τότε η απεικόνιση*

$$f^* : k[Y] \ni g \mapsto g \circ f \in k[X]$$

*είναι ομομορφισμός k-αλγεβρών.*

**Απόδειξη.** Η σύνθεση $g \circ f : X \to k$ είναι πολυωνυμική απεικόνιση και άρα είναι πολυωνυμική συνάρτηση, δηλαδή $g \circ f \in k[X]$. Η επαλήθευση ότι η $f^*$ είναι ομομορφισμός $k$-αλγεβρών είναι θέμα ρουτίνας: για παράδειγμα $f^*(g_1 g_2)(P) = [(g_1 g_2) \circ f](P) = (g_1 g_2)(f(P)) = g_1 f(P) g_2 f(P) = f^*(g_1)(P) f^*(g_2)(P) = (f^*(g_1) f^*(g_2))(P)$. Άρα $f^*(g_1 g_2) = f^*(g_1) f^*(g_2)$. □

Είναι ενδιαφέρον ότι ισχύει και το αντίστροφο του προηγούμενου λήμματος. Το επόμενο θεώρημα γενικεύει το Θεώρημα 2.3.2. Ουσιαστικά μας πληροφορεί ότι τα αλγεβρικά σύνολα προσδιορίζονται μονοσήμαντα (με προσέγγιση ισομορφισμού) από τους δακτυλίους των συντεταγμένων τους.

**8.3.4 Θεώρημα** *Έστω X, Y, Z, αλγεβρικά σύνολα.*

*(i)* *Αν* $f: X \to Y$ *και* $g: Y \to Z$ *είναι πολυωνυμικές απεικονίσεις τότε* $(g \circ f)^* = f^* \circ g^*$

*(ii)* *Κάθε ομομορφισμός k-αλγεβρών* $\varphi: k[Y] \to k[X]$ *είναι της μορφής* $\varphi = f^*$ *για μοναδική πολυωνυμική απεικόνιση* $f: X \to Y$.

*(iii)* *Η πολυωνυμική απεικόνιση* $f: X \to Y$ *είναι ισομορφισμός αν και μόνο αν ο ομομορφισμός* $f^*: k[Y] \to k[X]$ *είναι ισομορφισμός.*

**Απόδειξη.** (i) Αν $h \in k[Z]$, τότε $(g \circ f)^*(h) = h \circ (g \circ f) = (h \circ g) \circ f = f^*(h \circ g) = f^*(g^*(h)) = (f^* \circ g^*)(h)$.

(ii) και (iii) Η απόδειξη είναι παρόμοια με εκείνη του Θεωρήματος 2.3.2. □

Θα μελετήσουμε στη συνέχεια ρητές συναρτήσεις και ρητές απεικονίσεις.

Έστω $X \subseteq k^n$ ένα ανάγωγο αλγεβρικό σύνολο. Τότε το ιδεώδες $I(X)$ είναι πρώτο (Πρόταση 8.1.5). Συνεπώς ο δακτύλιος πηλίκο $k[x_1,...,x_n]/I(X)$ είναι περιοχή (Πρόταση 0.6.2), δηλαδή ο δακτύλιος συντεταγμένων $k[X]$ είναι περιοχή, και μπορούμε να θεωρήσουμε το σώμα πηλίκων του $k[X]$. Το σώμα αυτό συμβολίζεται με $k(X)$ και ονομάζεται *σώμα των ρητών συναρτήσεων* του *X*. Κάθε στοιχείο του $k(X)$ έχει τη μορφή $f/g$ με $f, g \in k[X]$ και $g \neq 0$. Ισχύει

$$\frac{f_1}{g_1} = \frac{f_2}{g_2} \Leftrightarrow f_1 g_2 - f_2 g_1 \in I(X).$$

Τα στοιχεία του $k(X)$ ονομάζονται *ρητές συναρτήσεις*. Όμως προσοχή: τα στοιχεία του $k(X)$ *δεν* είναι αναγκαστικά συναρτήσεις $X \to k$ λόγω των ριζών του παρονομαστή. Έτσι δίνουμε τον επόμενο ορισμό.

**8.3.5 Ορισμός** *Έστω $X$ ένα ανάγωγο αλγεβρικό σύνολο, $P \in X$ και $f \in k(X)$. Η ρητή συνάρτηση $f$ λέγεται κανονική στο $P$ αν υπάρχει παράσταση $f = g/h$ με $g, h \in k[X]$ και $h(P) \neq 0$.*

**8.3.6 Παράδειγμα** Έστω $X$ ο κύκλος $X = V(x^2 + y^2 - 1) \subseteq k^2$. Θεωρούμε τη ρητή συνάρτηση

$$f = \frac{1+y}{x}.$$

Προφανώς η $f$ είναι κανονική σε κάθε σημείο $P \in X$ με $P \neq (0,1), (0,-1)$. Όμως και στο $(0,-1)$ η $f$ είναι κανονική! Πράγματι,

$$f = \frac{x(1+y)}{x^2} = \frac{x(1+y)}{1-y^2} = \frac{x}{1-y}$$

και η ρητή συνάρτηση $x/1-y$ είναι προφανώς κανονική στο $(0,-1)$.

Το *πεδίο ορισμού* μιας ρητής συνάρτησης $f \in k(X)$ είναι το σύνολο

$$\text{dom } f = \{P \in X \mid f \text{ είναι κανονική στο } P\}.$$

Υπενθυμίζουμε από την Τοπολογία ότι ένα ανοικτό σύνολο ενός τοπολογικού χώρου λέγεται *πυκνό* αν έχει μη κενή τομή με κάθε μη κενό ανοικτό σύνολο.

**8.3.7 Θεώρημα** *Έστω $X$ ένα ανάγωγο αλγεβρικό σύνολο και $f \in k(X)$.*

*(i) Στην τοπολογία Zariski του $X$ το σύνολο* dom $f$ *είναι ανοικτό και πυκνό.*

*(ii) Έστω $k$ ένα αλγεβρικά κλειστό σώμα. Αν* dom $f = X$, *τότε $f \in k[X]$.*

**Απόδειξη.** (i) Το σύνολο (των "παρονομαστών" της $f$)

$$\Pi(f) = \left\{ h \in k[X] \mid \text{υπάρχει } g \in k[X] \text{ με } f = \frac{g}{h} \right\} \cup \{0\}$$

είναι ιδεώδες του $k[X]$. Ισχύει

$$X - \text{dom } f = V_X(\Pi(f)), \tag{11}$$

και συνεπώς το σύνολο dom $f$ είναι ανοικτό στην τοπολογία Zariski του $X$. Επιπλέον dom $f \neq \varnothing$. Τώρα σύμφωνα με την Άσκηση 16, κάθε μη κενό ανοικτό υποσύνολο ενός αναγώγου αλγεβρικού συνόλου είναι πυκνό.

(ii) Έχουμε $\text{dom}\, f = X \Leftrightarrow V(\Pi(f)) = \varnothing$ από την (11). Από το σχετικό Nullstellensatz $V_X(\Pi(f)) = \varnothing \Leftrightarrow \Pi(f) = k[X]$. Άρα $\text{dom}\, f = X \Leftrightarrow f \in k[X]$. □

Το προηγούμενο θεώρημα μας πληροφορεί ότι μια ρητή συνάρτηση $f \in k(X)$ είναι πολυωνυμική αν και μόνο αν είναι κανονική σε κάθε $P \in X$.

Θα μελετήσουμε τώρα ρητές απεικονίσεις μεταξύ αναγώγων αλγεβρικών συνόλων.

Για το σύνολο $A$ και $B$ θα λέμε ότι η $f : A \dashrightarrow B$ είναι μια *μερικώς ορισμένη απεικόνιση* αν η $f : A' \to B$ είναι απεικόνιση για κάποιο μη κενό υποσύνολο $A' \subseteq A$.

**8.3.8 Ορισμός** *Έστω* $X \subseteq k^n$, $Y \subseteq k^m$ *ανάγωγες ομοπαραλληλικές πολλαπλότητες.*

*(i) Μια μερικώς ορισμένη απεικόνιση* $f : X \dashrightarrow k^m$ *ονομάζεται ρητή απεικόνιση αν υπάρχουν ρητές συναρτήσεις* $f_1,..., f_m \in k(X)$ *με την ιδιότητα* $f(P) = (f_1(P),..., f_m(P))$ *για κάθε* $P \in \bigcap_i \text{dom}\, f_i$.

*Στην περίπτωση αυτή θέτουμε* $\text{dom}\, f = \bigcap_i \text{dom}\, f_i$.

*(ii) Έστω* ´$f : X \dashrightarrow k^m$ *μια ρητή απεικόνιση. Η f λέγεται κανονική στο* $P \in X$ *αν* $P \in \text{dom}\, f$.

*(iii) Μία ρητή απεικόνιση* $f : X \dashrightarrow Y$ *μεταξύ αναγώγων ομοπαραλληλικών πολλαπλοτήτων είναι μια ρητή απεικόνιση* $f : X \dashrightarrow k^m$ *για την οποία ισχύει* $f(\text{dom}\, f) \subseteq Y$.

**8.3.9 Παράδειγμα** Έστω $X = V(x^2 + y^2 - 1) \subseteq \mathbb{R}^2$ και $Y = \mathbb{R}$. Θέτοντας $f(a,b) = b/a$ για κάθε $(a,b) \in X$ με $a \neq 0$ ορίζεται μια ρητή απεικόνιση

$$f : X \dashrightarrow Y, \quad f(a,b) = \frac{b}{a}$$

με $\text{dom}\, f = V - \{(0,1),(0,-1)\}$. Επίσης μια ρητή απεικόνιση είναι η

$$g: Y \dashrightarrow X, \quad f(t) = \left( \frac{-2t}{1+t^2}, \frac{1-\lambda^2}{1+\lambda^2} \right)$$

(δες την § 2.1). Εδώ $\operatorname{dom} g = Y$, δηλαδή η $g$ είναι απεικόνιση. Ένα τρίτο παράδειγμα είναι η ρητή απεικόνιση

$$h: X \dashrightarrow Y, \quad h(a,b) = \frac{1+b}{a}.$$

Η $h$ είναι κανονική στο σημείο (0,–1) αν και $a = 0$ (δες το Παράδειγμα 8.3.6). Ισχύει $\operatorname{dom} h = X - \{(0,1)\}$.

Αν $f: X \dashrightarrow Y$ και $g: Y \dashrightarrow Z$ είναι ρητές απεικονίσεις αναγώγων ομοπαραλληλικών πολλαπλοτήτων, τότε γενικά δεν μπορεί να οριστεί η σύνθεση $g \circ f: X \to Z$ κατά τον προφανή τρόπο γιατί ενδέχεται $f(\operatorname{dom} f) \cap \operatorname{dom} g = \varnothing$. Έτσι φθάνουμε στον επόμενο ορισμό.

**8.3.10 Ορισμός** *Μια ρητή απεικόνιση $f: X \dashrightarrow Y$ λέγεται κυρίαρχη αν το σύνολο $f(\operatorname{dom} f)$ είναι πυκνό στο Y ως προς την τοπολογία Zariski.*

Τώρα αν $f: X \dashrightarrow Y$ και $g: Y \dashrightarrow Z$ είναι ρητές απεικονίσεις και η $f$ είναι κυρίαρχη, τότε το πυκνό σύνολο $f(\operatorname{dom} f)$ έχει μη κενή τομή με το σύνολο $\operatorname{dom} g$, γιατί το $\operatorname{dom} g$ είναι ανοικτό και μη κενό (Ορισμός 8.3.8 i)). Επομένως ορίζεται κατά τον προφανή τρόπο η σύνθεση.

$$g \circ f: X \dashrightarrow Z$$

που είναι βέβαια ρητή απεικόνιση.

Δίνουμε τώρα έναν αλγεβρικό χαρακτηρισμό κυρίαρχων ρητών απεικονίσεων.

**8.3.11 Πρόταση** *Έστω $f: X \dashrightarrow Y$ ρητή απεικόνιση αναγώγων ομοπαραλληλικών πολλαπλοτήτων*

*(i) Η απεικόνιση*

$$f^*: k[Y] \to k(X), \quad f^*(g) = g \circ f$$

*είναι ομομορφισμών k-αλγεβρών.*

*(ii) Η f είναι κυρίαρχη αν και μόνο αν η $f^*$ είναι μονομορφισμός.*

**Απόδειξη.** (i) Η απόδειξη είναι όμοια με αυτή του Λήμματος 8.3.3.

(ii) $\ker f^* = \{g \in k[Y] \mid g \circ f = 0\} = \{g \in k[Y] \mid f(\mathrm{dom}\, f) \subseteq V(g)\}$. Έστω $g \in \ker f^*$. Αν η $f$ είναι κυρίαρχη τότε το σύνολο $f(\mathrm{dom}\, f)$ είναι πυκνό στο $Y$. Επειδή $f(\mathrm{dom}\, f) \subseteq V(g)$ και το $V(g)$ είναι κλειστό συμπεραίνουμε ότι $Y(g) = Y$ (γιατί το πυκνό $f(\mathrm{dom}\, f)$ τέμνει το ανοικτό σύνολο $Y - V(g)$). Άρα $g = 0$. Αντίστροφα, έστω $\ker f^* = 0$. Έστω ότι το $f(\mathrm{dom}\, f)$ δεν είναι πυκνό στο $Y$. Τότε υπάρχει μη κενό ανοικτό σύνολο $Y - V(g)$, για κάποιο $g \in k[Y]$, με την ιδιότητα $f(\mathrm{dom}\, f) \cap (Y - V(g)) = \varnothing$. Δηλαδή $f(\mathrm{dom}\, f) \subseteq V(g)$. Αλλά τότε $g \in \ker f^* = 0$, οπότε $Y - V(g) = \varnothing$, άτοπο. □

Μια κυρίαρχη ρητή απεικόνιση $f : X \dashrightarrow Y$ αναγώγων αλγεβρικών συνόλων ονομάζεται *αμφίρητη ισοδυναμία* αν υπάρχει κυρίαρχη ρητή απεικόνιση $g : Y \dashrightarrow X$ με τις ιδιότητες $f \circ g = 1_Y$ και $g \circ f = 1_X$. Οι προηγούμενες ισότητες είναι ισότητες μερικώς ορισμένων συναρτήσεων. Έτσι $f \circ g = 1_Y$ σημαίνει ότι για κάθε $P \in \mathrm{dom}(f \circ g)$ ισχύει $(f \circ g)(P) = P$. Προφανώς κάθε ισομορφισμός $f : X \to Y$ είναι αμφίρητη ισοδυναμία, αλλά το αντίστροφο δεν ισχύει όπως θα δούμε παρακάτω.

Το επόμενο θεώρημα είναι το αντίστοιχο του Θεωρήματος 8.3.4 για ρητές απεικονίσεις και η απόδειξή του είναι παρόμοια.

**8.3.12 Θεώρημα** *Έστω X, Y, Z ανάγωγα αλγεβρικά σύνολα.*

*(i) Αν $f : X \dashrightarrow Y$ είναι κυρίαρχη ρητή απεικόνιση, τότε ο ομομορφισμός k-αλγεβρών $f^* : k[Y] \to k(X)$ επάγει έναν k-ομομορφισμό σωμάτων*

$$f^* : k(Y) \ni \frac{g}{h} \mapsto \frac{f^*(g)}{f^*(h)} \in k(X), \quad g, h \in k[Y], \quad h \neq 0.$$

*(ii) Κάθε k-ομομορφισμός σωμάτων $\varphi : k(Y) \to k(X)$ είναι της μορφής $\varphi = f^*$ για μοναδική κυρίαρχη ρητή απεικόνιση $f : X \dashrightarrow Y$.*

*(iii) Αν $f : X \dashrightarrow Y$ και $g : Y \dashrightarrow Z$ είναι κυρίαρχες ρητές απεικονίσεις τότε $(g \circ f)^* = f^* \circ g^*$.*

*(iv) Η κυρίαρχη ρητή απεικόνιση* $f : X \dashrightarrow Y$ *είναι αμφίρητη ισοδυναμία αν και μόνο αν ο k-ομομορφισμός* $f^* : k(Y) \to k(X)$ *είναι ισομορφισμός.*

**Απόδειξη.** (i) Εφόσον η *f* είναι κυρίαρχη, $\ker f^* = 0$ (Πρόταση 8.3.11(ii)). Άρα για $h \in k[Y]$ με $h \neq 0$ έχουμε $f^*(h) \neq 0$ και συνεπώς η απεικόνιση $f^* : k(Y) \to k(X)$ είναι καλά ορισμένη. Παραλείπουμε την επαλήθευση ότι η $f^*$ είναι k-ομομορφισμός, γιατί είναι απλούστατο θέμα ρουτίνας.

(ii) Η απόδειξη δεν διαφέρει ουσιαστικά από την απόδειξη του Θεωρήματος 8.3.4 με την παρατήρηση ότι η *f* είναι κυρίαρχη λόγω της Πρότασης 8.3.11(ii).

(iii) Έπεται από τους ορισμούς.

(iv) Έπεται από τις (ii) και (iii) και το γεγονός ότι $(1_X)^* = 1_{k(X)}$. □

Για παράδειγμα, αν $X \subseteq k^2$ είναι η κυβική που ορίζεται από $y^2 = x^3$, τότε η απεικόνιση $k \to X$, $t \mapsto (t^2, t^3)$ είναι αμφίρητη ισοδυναμία, αλλά όχι ισομορφισμός (γιατί; δες και § 2.3).

## Ασκήσεις

Στις παρακάτω ασκήσεις το *k* είναι πάντοτε *αλγεβρικά κλειστό*.

**1.** Μια *k*-άλγεβρα είναι δακτύλιος συντεταγμένων μιας ομοπαραλληλικής πολλαπλότητας αν και μόνο αν είναι πεπερασμένα παραγόμενη και δεν έχει μηδενικά μηδενοδύναμα στοιχεία.

**2.** *Πρώτη εικασία του A. Weil.* Έστω *k* ένα σώμα χαρακτηριστικής $p > 0$. Έστω $X \subseteq k^n$ που ορίζεται από πολυώνυμα $f_i \in \mathbb{Z}_p[x_1, ..., x_n]$.

(i) Η απεικόνιση $F^r : X \ni (a_1, ..., a_n) \mapsto (a_1^{p^r}, ..., a_n^{p^r}) \in k^n$, όπου $r \in \mathbb{N}$, είναι κανονική και $\mathrm{Im} F^r \subseteq X$.

(ii) Θέτοντας $v^r = \#\{P \in X \mid F^r(P) = P\}$ ορίζουμε την τυπική δυναμοσειρά

$$P_X(t) = \sum_{r=1}^{\infty} v^r t^r \in \mathbb{Z}[[t]].$$

Για $X = k^n$, αποδείξετε ότι

$$P_X(t) = \frac{p^n t}{1 - p^n t} \in \mathbb{Z}(t).$$

(iii) Ποια είναι η $P_X(t)$, όπου $X \subseteq k^2$ είναι η έλλειψη

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1;$$

Ισχύει $P_X(t) \in \mathbb{Z}(t)$;

Η πρώτη εικασία του A. Weil, ισχυρίζεται ότι $P_X(t) \in \mathbb{Z}(t)$, δηλαδή η $P_X(t)$ είναι ρητή συνάρτηση του *t*. Ο ίδιος ο Weil απέδειξε την εικασία για καμπύλες το 1948. Ο Dwork απέδειξε γενικά την εικασία το 1960.

**3.** Έστω το ιδεώδες $J = (x^2 + y^2 - 1, y - 1)$ του $k[x, y]$. Βρείτε ένα $f \in I(V(J)) - J$.

**4.** Έστω το ιδεώδες $J = (xy, yz, xz)$ του $k[x, y, z]$. Ποιο είναι το σύνολο $V(J)$; Είναι ανάγωγο; Ισχύει $J = I(V(J))$; Αποδείξετε ότι το *J* δεν παράγεται από 2 στοιχεία.

**5.** Έστω $f = x^2 - y^2$ και $g = x^3 + xy^2 - y^3 - x^2 y - x + y \in \mathbb{C}[x, y]$. Προσδιορίσετε τις ανάγωγες συνιστώσες του $V(f, g)$.

**6.** Δώστε μια νέα απόδειξη του Πορίσματος 2.1.6.

**7.** Κάθε ισομορφισμός $f : k \to k$ είναι της μορφής $f(x) = ax + b$, $a \neq 0$.

**8.** Έστω $f : X \to Y$ μια κανονική απεικόνιση. Το σύνολο

$$\Gamma_f = \{(a, f(a)) \in X \times Y \mid a \in X\}$$

ονομάζεται γράφημα της *f*. Αποδείξετε ότι $(a)\Gamma_f \subseteq X \times Y$ είναι κλειστό σύνολο και $(b)\Gamma_f$ είναι ισόμορφο με το *X*.

**9.** Αποδείξετε για κάθε κανονική απεικόνιση $f : X \times Y$ υπάρχει κανονική απεικόνιση $g : X \to X \times Y$ που δίνει έναν ισομορφισμό $X \cong \operatorname{Im} g$, τέτοιον ώστε $f = \Pi_Y \circ g$, όπου $\Pi_Y(x, y) = y$.

**10.** Έστω $k$ σώμα χαρακτηριστικώς $\neq 2$. Έστω $X$ η κυβική που ορίζεται από $y^2 = x^2 + x^3$. Είναι η $X$ ισόμορφη με την ευθεία; Αμφίρητα ισοδύναμη;

**11.** Έστω $X \subseteq k^3$ που ορίζεται από $y^2 = xz$ και $z^2 = y^3$. Ποιες είναι οι ανάγωγες συνιστώσες του $X$; Αποδείξετε ότι κάθε μια είναι αμφίρητα ισοδύναμη με την ευθεία.

**12.** Σε ποια σημεία της κυβικής $X$ που ορίζεται από $y^2 = x^2 + x^3$ η ρητή συνάρτηση $t = y/x$ είναι κανονική; Αποδείξετε ότι $y/x \notin k[X]$.

**13.** Η τοπολογία Zariski δεν είναι γενικά Hausdorff.

**14.** Έστω $X \subseteq k^2$ που ορίζεται από $y^3 = x^4 + x^3$. Αποδείξετε ότι υπάρχει ρητή απεικόνιση $\psi : X - - \to k$, $\psi(x,y) = x/y$. Η αντίστροφη είναι πολυωνυμική $\varphi : k \to X$. Η $\varphi$ δίνει έναν ισομορφισμό $k$-{τρία σημεία} $\cong X - \{0,0\}$.

**15.** Έστω $X \subseteq k^3$ που ορίζεται από $y^2 + z^2 = x^3$. Αποδείξετε ότι το $X$ είναι ανάγωγο και αμφίρητα ισοδύναμο με το επίπεδο $k^2$.

**16.** Έστω $X \subseteq k^n$ μια ανάγωγη ομοπαραλληλική πολλαπλότητα. Τότε κάθε μη κενό ανοικτό σύνολο του $X$ είναι πυκνό στο $X$ ως προς την τοπολογία Zariski.

**17.** Έστω $X \subseteq k^n$ μια ανάγωγη ομοπαραλληλική πολλαπλότητα που ορίζεται από $f = 0$. Ένα σημείο $P \in X$ λέγεται ιδιάζον αν μηδενίζει τις μερικές παραγώγους, δηλαδή αν $(\partial f / \partial x_i)(P) = 0$ για κάθε $i$. Με $X_0$ συμβολίζουμε το συμπλήρωμα στο $X$ του συνόλου των ιδιαζόντων σημείων. Αποδείξετε ότι το $X_0$ είναι ανοικτό και πυκνό στο $X$ ως προς την τοπολογία Zariski.

Υπόδειξη: το σύνολο των ιδιαζόντων σημείων $X_{\sin}$ ορίζεται από τα πολυώνυμα $f, \partial f/\partial x_i, ..., \partial f/\partial x_n$. Αρκεί (Άσκηση 16) να δειχθεί ότι $X_{\sin} \neq \varnothing$. Έστω $X_{\sin} = \varnothing$ και αποδείξετε ότι $f =$ σταθερά (αν η χαρακτηριστική του $k$ είναι 0) ή $f = p$-στή δύναμη (αν η χαρακτηριστική του $k$ είναι $p > 0$). Αυτό είναι άτοπο.

**18.** Ποια είναι τα πρώτα και μέγιστα ιδέωδη του $k[x,y]$; (Υπόδειξη: δες την § 1.4).

**19.** Έστω $k$ σώμα χαρακτηριστικής $p > 0$. Η απεικόνιση

$$k \ni a \mapsto a^p \in k$$

*(μορφισμός του Frobenius)* είναι πολυωνυμική, $1-1$ και επί αλλά *δεν* είναι ισομορφισμός. (Δες και την Άσκηση 7).

**20.** Οι ανάγωγες συνιστώσες αλγεβρικού συνόλου είναι μοναδικές. Υπόδειξη: Έστω $X = X_1 \cup \cdots \cup X_m$ και $Y = Y_1 \cup \cdots \cup Y_n$ με $X_i, Y_j$ ανάγωγα και $X_i \not\subseteq X_j$, $Y_i \not\subseteq Y_j$ για $i \neq j$. Τότε $X_i = X_i \cap X = (X_i \cap Y_1) \cup \cdots \cup (X_i \cap Y_n) \Rightarrow X_i \subseteq Y_j$ για κάποιο $j$. Όμοια $Y_j \subseteq X_{i'}$ για κάποιο $i'$. Άρα $i = i'$ και $X_i = Y_j$.

# Κεφάλαιο 9

# Αλγεβρικοί Ακέραιοι

Στο Κεφάλαιο αυτό μελετάμε αλγεβρικούς ακεραίους στο $\mathbb{C}$. Το κύριο αποτέλεσμα μας πληροφορεί ότι ο δακτύλιος των αλγεβρικών ακεραίων αριθμητικού σώματος είναι της Noether. Επίσης εξετάζονται οι έννοιες της ακέραιας βάσης και διακρίνουσας αριθμητικού σώματος.

## 9.1 Αριθμητικά Σώματα

Αν το $k$ είναι υπόσωμα του σώματος $K$ θα λέμε ότι το $K$ είναι *επέκταση* του $k$. Συμβολικά θα γράφουμε $K/k$.

Έστω επέκταση σωμάτων $K/k$. Το $K$ είναι ένας $k$-διανυσματικός χώρος κατά τον προφανή τρόπο. Η διάστασή του συμβολίζεται με $[K:k]$ και ονομάζεται *βαθμός* της επέκτασης $K/k$, δηλαδή

$$[K:k] = \dim_k K .$$

Έστω επέκταση σωμάτων $K/k$ και στοιχεία $a_1,...,a_n \in K$. Με $k(a_1,...,a_n)$ συμβολίζουμε την τομή όλων των υποσωμάτων του $K$ που περιέχουν το $k$ και τα $a_1,...,a_n$. Έτσι το $k(a_1,...,a_n)$ είναι το μικρότερο υπόσωμα του $K$ που περιέχει το $k$ και τα $a_1,...,a_n$.

**9.1.1 Πρόταση** *Έστω $K/k$ επέκταση σωμάτων και στοιχεία $a_1,...,a_n \in K$. Τότε*

$$k(a_1,...,a_n) = \left\{ \frac{f(a_1,...,a_n)}{g(a_1,...,a_n)} \in K \mid f(x_1,...,x_n), g(x_1,...,x_n) \in k[x_1,...,x_n], g(a_1,...,a_n) \neq 0 \right\}$$

**Απόδειξη.** Παρόμοια με την απόδειξη της Πρότασης 0.2.3. □

Μια επέκταση σωμάτων $K/k$ ονομάζεται *πεπερασμένη* αν $[K:k]<\infty$. Κάθε πεπερασμένη επέκταση $K/\mathbb{Q}$ του σώματος $\mathbb{Q}$ των ρητών αριθμών ονομάζεται *αριθμητικό σώμα*. Το επόμενο θεώρημα μας πληροφορεί ότι κάθε αριθμητικό σώμα $K$ έχει μια απλή μορφή, που θα φανεί χρήσιμη στα παρακάτω.

**9.1.2 Θεώρημα** *Έστω $K$ αριθμητικό σώμα. Τότε υπάρχει $\theta\in K$ έτσι ώστε*

$$K=\mathbb{Q}(\theta).$$

Για την απόδειξη θα χρειαστούμε την έννοια του ελάχιστου πολυωνύμου και ένα απλό λήμμα που δίνουμε αμέσως παρακάτω.

Έστω $K/k$ μια πεπερασμένη επέκταση σωμάτων και $a\in K$. Θεωρούμε τον επιμορφισμό δακτυλίων

$$\varphi: k[x] \ni f(x)\mapsto f(a)\in k[a].$$

Ισχύει $\ker\varphi\neq 0$, γιατί τα στοιχεία $1=a^0,a^1,a^2,...,a^n$, όπου $n=[K:k]$, είναι γραμμικά εξαρτημένα πάνω από το $k$, αφού το πλήθος τους είναι $n+1>n$. Επειδή ο $k[x]$ είναι δακτύλιος κυρίων ιδεωδών (Παράδειγμα 1.1.6), έχουμε $\ker\varphi=(p(x))$ για κάποιο $p(x)\in k[x]$. Μπορούμε να υποθέσουμε ότι το $p(x)$ είναι μονικό. Ισχύει $k[x]/(p(x))\cong k[a]$ (Θεώρημα 0.3.2), και επειδή το $k[a]$ είναι ακέραια περιοχή (γιατί περιέχεται στο $K$ που είναι σώμα) συμπεραίνουμε ότι το $(p(x))$ είναι πρώτο ιδεώδες (Πρόταση 0.6.2). Άρα το $p(x)$ είναι ανάγωγο στο $k[x]$. Το μονοσήμαντα ορισμένο ανάγωγο μονικό πολυώνυμο $p(x)\in k[x]$ *ελάχιστο πολυώνυμο* του $a$ πάνω από το $k$. Συμβολίζεται με $\mathrm{Irr}(a,k)=p(x)$. Φυσικά αν $f(a)=0$ για κάποιο $f(x)\in k[x]$ τότε το $\mathrm{Irr}(a,k)$ διαιρεί το $f(x)$ στο $k[x]$, γιατί $f(a)=0\Rightarrow f(x)\in\ker\varphi$.

**9.1.3 Λήμμα** *Έστω $k$ ένα υπόσωμα του σώματος $\mathbb{C}$ των μιγαδικών αριθμών και $p(x)\in k[x]$ ένα ανάγωγο πολυώνυμο. Τότε κάθε ρίζα του $p(x)$ στο $\mathbb{C}$ είναι απλή.*

**Απόδειξη.** Έστω $p'(x)$ η παράγωγος του $p(x)$. Ισχύει $p'(x)\neq 0$. Στο $k[x]$ ισχύει μ.κ.δ. $(p(x),p'(x))=1$, γιατί το $p(x)$ είναι ανάγωγο και δεν διαιρεί το $p'(x)$ αφού $\deg p(x)>\deg p'(x)$. Τώρα από τη σχέση μ.κ.δ. $(p(x),p'(x))=1$ και την Άσκηση 1.13 συμπεραίνουμε ότι υπάρχουν $a(x),b(x)\in k[x]$ με την ιδιότητα

$$p(x)a(x) + p'(x)b(x) = 1. \qquad (1)$$

Αν $c$ είναι διπλή ρίζα του $p(x)$ στο $\mathbb{C}$ τότε $(x-c)^2 \mid p(x)$ στο $\mathbb{C}[x]$ και συνεπώς $x-c \mid p'(x)$ στο $\mathbb{C}[x]$. Λόγω της (1) καταλήγουμε σε άτοπο. □

**Απόδειξη του Θεωρήματος 9.1.2.**

Εφόσον $[K:\mathbb{Q}] < \infty$, υπάρχουν $a_1,...,a_n \in K$ με την ιδιότητα $K = \mathbb{Q}(a_1,...,a_n)$ (για παράδειγμα, κάθε βάση $\{a_1,...,a_n\}$ του $k$-διανυσματικού χώρου $K$ έχει την προηγούμενη ιδιότητα). Αρκεί επομένως να αποδείξουμε ότι: αν $K = k(a,b)$ με $a,b \in K$ και $k$ υπόσωμα του $K$, τότε υπάρχει $\theta \in K$ με την ιδιότητα $K = k(\theta)$. (Το ζητούμενο προκύπτει από διαδοχική εφαρμογή της ανωτέρω συνεπαγωγής).

Έστω $p(x) = \mathrm{Irr}(a,k)$ και $q(x) = \mathrm{Irr}(b,k)$. Θεωρούμε επίσης τις παραγοντοποιήσεις στο $\mathbb{C}$

$$p(x) = (x-a_1)\cdots(x-a_n),\ q(x) = (x-b_1)\cdots(x-b_m)$$

όπου $a_1 = a$ και $b_1 = b$.

Τα $b_j$ είναι διαφορετικά ανά δύο λόγω του Λήμματος 9.1.3. Θεωρούμε τα στοιχεία

$$\frac{a_i - a_1}{b_1 - b_j} \in \mathbb{C} \qquad (2)$$

όπου $j \neq 1$. Επειδή το $k$ είναι άπειρο σώμα και τα στοιχεία στην (2) είναι πεπερασμένου πλήθους, υπάρχει $c \in k - \{0\}$ με $c$ διάφορο από κάθε στοιχείο στη (2). Θέτουμε

$$\theta = a + cb. \qquad (3)$$

Θα αποδείξουμε ότι $k(a,b) = k(\theta)$. Η σχέση $k(\theta) \subseteq k(a,b)$ είναι προφανής. Αρκεί να δείξουμε ότι $a,b \in k(\theta)$ και για τούτο αρκεί να δείξουμε ότι $b \in k(\theta)$ λόγω της (3).

Θεωρούμε το πολυώνυμο

$$r(x) = p(\theta - cx) \in k(\theta)[t].$$

Ισχύει $r(b) = p(\theta - cb) = p(a) = 0$. Έτσι το $b$ είναι κοινή ρίζα των πολυωνύμων $r \in k(\theta)[t]$ και $q \in k[t] \subseteq k(\theta)[t]$. Επομένως

$$\mathrm{Irr}(b,k(\theta))\,|\,r \quad \text{και} \quad \mathrm{Irr}(b,k(\theta))\,|\,q\,. \tag{4}$$

*Ισχυρισμός*. Τα πολυώνυμα $r$ και $q$ έχουν ακριβώς μια κοινή ρίζα στο $\mathbb{C}$. Πράγματι, αν $\rho$ είναι ρίζα του $r$, το $\theta - c\rho$ είναι ρίζα του $p$ και άρα

$$\theta - c\rho \in \{a_1,...,a_n\}\,.$$

Όμως $\rho$ ρίζα του $q$ σημαίνει

$$\rho \in \{b_1,...,b_m\}\,.$$

Οι δύο παραπάνω συνθήκες και ο ορισμός του $c$ δίνουν $\rho = b$.

Από τον ισχυρισμό και την (4) έπεται ότι

$$\mathrm{Irr}(b,k(\theta)) = x + d$$

όπου $d \in k(\theta)$. Άρα $b + d = 0$ δηλαδή $b = -d \in k(\theta)$. □

**9.1.4 Παράδειγμα** Έστω $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Τότε

$$\mathrm{Irr}(\sqrt{2},\mathbb{Q}) = x^2 - 2$$

$$\mathrm{Irr}(\sqrt{3},\mathbb{Q}) = x^2 - 3\,.$$

Άρα $a_1 = \sqrt{2}$, $a_2 = -\sqrt{2}$, $b_1 = \sqrt{3}$, $b_2 = -\sqrt{3}$. Το θεώρημα (ή μάλλον η απόδειξή του) μας πληροφορεί ότι για κάθε $c \in \mathbb{Q} - \{0\}$ με

$$c \neq \frac{-\sqrt{2} - \sqrt{2}}{\sqrt{3} - (-\sqrt{3})} = -\frac{\sqrt{2}}{\sqrt{3}}\,,$$

δηλαδή για κάθε $c \in \mathbb{Q} - \{0\}$, ισχύει $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2} + c\sqrt{3})$. Για παράδειγμα μπορούμε να πάρουμε $c = 1$, οπότε

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})\,.$$

Φυσικά η τελευταία ισότητα αποδεικνύεται εύκολα χωρίς τη χρήση του θεωρήματος (πως;).

**Σημείωση.** Οι αναγνώστες που είναι έμπειροι στη θεωρία Galois θα αναγνωρίσουν την έννοια της διαχωρισιμότητας που υπεισέρχεται στο Θεώρημα 9.1.2 και στο Λήμμα 9.1.3.

Αν $K = \mathbb{Q}(\theta)$ είναι ένα αριθμητικό σώμα τότε ο βαθμός της επέκτασης $K/\mathbb{Q}$ είναι $[K:\mathbb{Q}] = n$ όπου $n$ είναι ο βαθμός του πολυωνύμου $\mathrm{Irr}(\theta,\mathbb{Q})$. Πράγματι, τα

στοιχεία $1,\theta,\theta^2,...,\theta^{n-1}$ είναι μια βάση του $K$ ως $\mathbb{Q}$-διανυσματικός χώρος: είναι γραμμικώς ανεξάρτητα, γιατί αν $a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}=0$ τότε το πολυώνυμο $a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ μηδενίζεται από το $\theta$ και έχει βαθμό μικρότερο από το $n$. Άρα είναι το μηδενικό πολυώνυμο. Αν $\mathrm{Irr}(\theta,\mathbb{Q})=c_0+c_1x+\cdots+x^n$, τότε $c_0+c_1\theta+\cdots+\theta^n=0\Rightarrow\theta^n=-(c_{n-1}\theta^{n-1}+\cdots+c_1\theta+c_0)$. Από την τελευταία σχέση συμπεραίνουμε ότι για κάθε $m>0$, το $\theta^{n+m}$ είναι γραμμικός συνδυασμός των $1,\theta,...,\theta^{n-1}$. Άρα τα $1,\theta,...,\theta^{n-1}$ παράγουν το $K$. Έχουμε αποδείξει την ακόλουθη πρόταση:

**9.2.5 Πρόταση** *Έστω $K=\mathbb{Q}(\theta)$ ένα αριθμητικό σώμα και $n$ ο βαθμός του πολυωνύμου $\mathrm{Irr}(\theta,\mathbb{Q})$. Τότε μία βάση του $K$ ως $\mathbb{Q}$-διανυσματικός χώρος είναι το σύνολο $\{1,\theta,...,\theta^{n-1}\}$.*

## 9.2 Διακρίνουσα Βάσης

Σε κάθε βάση ενός αριθμητικού σώματος θα ορίσουμε στην παράγραφο αυτή έναν ρητό αριθμό που ονομάζεται διακρίνουσα. Η έννοια αυτή θα βρει εφαρμογή στην επόμενη παράγραφο όπου μελετούμε ακέραιες βάσεις.

Έστω $K$ ένα αριθμητικό σώμα. Μας ενδιαφέρουν οι μονομορφισμοί σωμάτων $K\to\mathbb{C}$. Η επόμενη πρόταση μας πληροφορεί ότι το πλήθος τους είναι πεπερασμένο και μάλιστα ίσο με $[K:\mathbb{Q}]$. Πρώτα μια παρατήρηση: αν $\sigma:\mathbb{Q}(\theta)\to\mathbb{C}$, όπου $\theta\in\mathbb{C}$ είναι αλγεβρικό, είναι ομομορφισμός σωμάτων, τότε ο $\sigma$ προσδιορίζεται πλήρως από την εικόνα $\sigma:\mathbb{Q}(\theta)\to\mathbb{C}$ έχει $\ker\sigma=0$ ή $\ker\sigma=\mathbb{Q}(\theta)$ αφού το $\ker\sigma$ είναι ιδεώδες του σώματος $\mathbb{Q}(\theta)$. Υποθέτουμε λοιπόν $\sigma\neq 0$. Κάθε ομομορφισμός $\sigma:\mathbb{Q}(\theta)\to\mathbb{C}$ είναι σταθερός στο $\mathbb{Q}$, δηλαδή $\sigma(a)=a$ για κάθε $a\in\mathbb{Q}$, γιατί: $\sigma(a)=\sigma(a\cdot 1)=\sigma(a)\sigma(1)\Rightarrow\sigma(1)=1\Rightarrow\sigma(m)=\sigma(1+\cdots+1)=m\sigma(1)=m$ για κάθε $m\in\mathbb{Z}$. Τέλος

$$\sigma\left(\frac{m}{m'}\right)=\frac{\sigma(m)}{\sigma(m')}=\frac{m}{m'},$$

για κάθε $m, m' \in \mathbb{Z}$, $m' \neq 0$. Τώρα κάθε $b \in \mathbb{Q}(\theta)$ γράφεται ως $b = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$ (Πρόταση 9.1.5). Επομένως για τον ομομορφισμό $\sigma$ ισχύει $\sigma(b) = a_0 + a_1\sigma(\theta) + \cdots + \sigma(\theta)^{n-1}$. Άρα κάθε ομομορφισμός $\sigma : \mathbb{Q}(\theta) \to \mathbb{C}$ ορίζεται μονοσήμαντα από την εικόνα $\sigma(\theta)$.

**9.2.1 Πρόταση** *Έστω $K = \mathbb{Q}(\theta)$ ένα αριθμητικό σώμα βαθμού $n$ και έστω $\theta_1, ..., \theta_n \in \mathbb{C}$ οι ρίζες του πολυωνύμου $\mathrm{Irr}(\theta, \mathbb{Q})$. Τότε για κάθε $i = 1, ...., n$ υπάρχει μονομορφισμός σωμάτων $\sigma_i : K \to \mathbb{C}$ που ικανοποιεί*

$$\sigma_i(\theta) = \theta_i .$$

*Οι μονομορφισμοί $\sigma_1, ...., \sigma_n$ είναι διακεκριμένοι. Αντίστροφα, κάθε μονομορφισμός $K \to \mathbb{C}$ είναι ένας από τους $\sigma_i$.*

**Απόδειξη.** Έστω $p(x) = \mathrm{Irr}(\theta, \mathbb{Q})$. Ο επιμορφισμός δακτυλίων

$$\mathbb{Q}[x] \ni f(x) \mapsto f(\theta) \in \mathbb{Q}[\theta]$$

επάγει έναν ισομορφισμό δακτυλίων $\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}[\theta]$. Το αριστερό σκέλος είναι σώμα, γιατί ο $\mathbb{Q}[x]$ είναι δακτύλιος κυρίων ιδεωδών και το $p(x)$ είναι ανάγωγο (Λήμμα 1.2.4). Άρα το $\mathbb{Q}[\theta]$ είναι σώμα. Επειδή $\theta \in \mathbb{Q}[\theta] \subseteq \mathbb{Q}(\theta)$, ο ορισμός του $\mathbb{Q}[\theta]$ δίνει $\mathbb{Q}[\theta] = \mathbb{Q}(\theta)$. Έτσι για κάθε $i = 1, ..., n$ ο ομομορφισμός δακτυλίων

$$\mathbb{Q}[x] \ni f(x) \mapsto f(\theta_i) \in \mathbb{Q}(\theta_i)$$

επάγει έναν ισομορφισμό σωμάτων

$$\mathbb{Q}[x]/(p_i(x)) \cong \mathbb{Q}(\theta_i),$$

όπου $p_i(x) = \mathrm{Irr}(\theta_i, \mathbb{Q})$. Όμως $p(\theta_i) = 0 \Rightarrow p_i(x)$ διαιρεί το $p(x) \Rightarrow p_i(x) = p(x)$ γιατί το $p(x)$ είναι ανάγωγο και τα $p_i(x)$, $p(x)$ είναι μονικά. Με $\sigma_i$ συμβολίζουμε τον μονομορφισμό που είναι η σύνθεση

$$\sigma_i : \mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(p_i(x)) \cong \mathbb{Q}(\theta_i) \subseteq \mathbb{C}.$$

Ισχύει $\sigma_i(\theta) = \theta_i$. Από το Λήμμα 9.1.3 τα $\theta_i$ είναι διάφορα ανά δύο. Άρα και οι $\sigma_i$ είναι διάφοροι ανά δύο.

Αντίστροφα, έστω $\sigma:\mathbb{Q}(\theta)\to\mathbb{C}$ μονομορφισμός. Τότε $p(\theta)=0\Rightarrow \sigma(p(\theta))=0\Rightarrow p(\sigma(\theta))=0$, γιατί $\sigma(a)=a$ για κάθε $a\in\mathbb{Q}$ όπως παρατηρήσαμε πριν την Πρόταση 9.1.1. Άρα $\sigma(\theta)=\theta_i$ για κάποιο *i*. □

Για παράδειγμα οι μονομορφισμοί $\mathbb{Q}(\sqrt{2})\to\mathbb{C}$ είναι

$$\sigma_1:\mathbb{Q}(\sqrt{2})\to\mathbb{C},\quad \sigma_1(\sqrt{2})=\sqrt{2}$$
$$\sigma_2:\mathbb{Q}(\sqrt{2})\to\mathbb{C},\quad \sigma_2(\sqrt{2})=-\sqrt{2}$$

γιατί $\mathrm{Irr}(\sqrt{2},\mathbb{Q})=x^2-2$. Έτσι το τυχαίο $a_0+a_1\sqrt{2}\in\mathbb{Q}(\sqrt{2})$ έχουμε $\sigma_1(a_0+a_1\sqrt{2})=a_0+a_1\sqrt{2}$ και $\sigma_2(a_0+a_1\sqrt{2})=a_0-a_1\sqrt{2}$. Παρόμοια, οι μονομορφισμοί $\mathbb{Q}(\sqrt[3]{2})\to\mathbb{C}$ είναι τρεις (γιατί $\mathrm{Irr}(\sqrt[3]{2},\mathbb{Q})=x^3-2$ από το κριτήριο του Eisenstein) που προσδιορίζονται από

$$\tau_1(\sqrt[3]{2})=\sqrt[3]{2}$$
$$\tau_2(\sqrt[3]{2})=\omega\sqrt[3]{2}$$
$$\tau_3(\sqrt[3]{2})=\omega^2\sqrt[3]{2},$$

όπου $\omega$ είναι ρίζα του πολυωνύμου $x^2+x+1$ (ή ισοδύναμα $\omega^3=1$ και $\omega\neq 1$).

**9.2.2 Ορισμός** *Έστω K ένα αριθμητικό σώμα βαθμού n και $a_1,a_2,...,a_n$ μία βάση του K ως $\mathbb{Q}$-διανυσματικός χώρος. Θεωρούμε τους μονομορφισμούς $\sigma_1,...,\sigma_n: K\to\mathbb{C}$ της Πρότασης 9.2.1 και τον $n\times n$ πίνακα στοιχείων του $\mathbb{C}$*

$$(\sigma_i(a_j))=\begin{pmatrix}\sigma_1(a_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(a_n)\\ & \cdots & & \\ \sigma_n(a_1) & \sigma_n(a_2) & \cdots & \sigma_n(a_n)\end{pmatrix}.$$

*Η διακρίνουσα της βάσης $a_1,...,a_n$ είναι ο μιγαδικός αριθμός*

$$\Delta(a_1,...,a_n)=(\det(\sigma_i(a_j)))^2.$$

Συνεχίζοντας το παραπάνω παράδειγμα έχουμε στο $\mathbb{Q}(\sqrt{2})$

$$\Delta(1,\sqrt{2})=\left(\det\begin{pmatrix}1 & \sqrt{2}\\ 1 & -\sqrt{2}\end{pmatrix}\right)^2=8,$$

και στο $\mathbb{Q}(\sqrt[3]{2})$

$$\Delta(1,\sqrt[3]{2},\sqrt[3]{4}) = \det\begin{pmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ 1 & \omega\sqrt[3]{2} & \omega^2\sqrt[3]{4} \\ 1 & \omega^2\sqrt[3]{2} & \omega\sqrt[3]{4} \end{pmatrix} = (\text{Vandermonde})$$

$$(\sqrt[3]{2}-\omega\sqrt[3]{2})^2(\sqrt[3]{2}-\omega^2\sqrt[3]{2})^2(\omega\sqrt[3]{2}-\omega^2\sqrt[3]{2})^2 = 4\omega^2(1-\omega)^4(1-\omega^2) = 108.$$

Δεν είναι τυχαίο το γεγονός στο προηγούμενο παράδειγμα ότι οι διακρίνουσες είναι ρητοί αριθμοί: Κάθε διακρίνουσα είναι ρητός αριθμός (δες την επόμενη πρόταση). Συχνά, αλλά όχι πάντα, είναι ακέραιος (δες την Πρόταση 9.3.3).

**9.2.3 Πρόταση** *Κάθε διακρίνουσα βάσης αριθμητικού σώματος είναι μη μηδενικός ρητός αριθμός.*

**Απόδειξη.** Έστω $K$ αριθμητικό σώμα. Ως συνήθως γράφουμε $K = \mathbb{Q}(\theta)$ (Θεώρημα 9.1.2). Έστω $\theta_1,...,\theta_n$ οι ρίζες του $\mathrm{Irr}(\theta,\mathbb{Q})$ στο $\mathbb{C}$. Θεωρούμε τη βάση $1,\theta,\theta^2,...,\theta^{n-1}$ του $K$ (Πρόταση 9.1.5). Από τον ορισμό της διακρίνουσας και την Πρόταση 9.2.1 παίρνουμε

$$\Delta(1,\theta,...,\theta^{n-1}) = \det(\theta_i^j), \quad i = 1,...,n, \quad j = 0,...,n-1.$$

Η ορίζουσα

$$\det(\theta_i^j) = \det\begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ & & \cdots & & \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{pmatrix}$$

είναι η γνωστή ορίζουσα Vandermonde. Άρα

$$\Delta(1,\theta,...,\theta^{n-1}) = \prod_{r<s}(\theta_r-\theta_s)^2. \tag{5}$$

Το δεξί σκέλος της (5) είναι συμμετρικό ως προς τα $\theta_i$. Από το θεμελιώδες θεώρημα των συμμετρικών πολυωνύμων (Θεώρημα 0.9.1) το δεξί σκέλος είναι πολυώνυμο στα στοιχειώδη συμμετρικά πολυώνυμα $e_1 = \theta_1 + \cdots + \theta_n$, $e_2 = \theta_1\theta_2 + \theta_1\theta_3 + \cdots + \theta_{n-1}\theta_n,...,e_n = \theta_1\cdots\theta_n$. Από τους τύπους του Vieta έχουμε $e_i = \pm p_{n-i}$ όπου $\mathrm{Irr}(\theta,\mathbb{Q}) = p_0 + p_1x + \cdots + p_{n-1}x^{n-1} + x^n$. Φυσικά $p_i \in \mathbb{Q}$. Άρα και $\Delta(1,\theta,...,\theta^{n-1}) \in \mathbb{Q}$. Από την (5) και το Λήμμα 9.1.3 έχουμε $\Delta \neq 0$.

Αποδείξαμε λοιπόν τον ισχυρισμό της πρότασης για την συγκεκριμένη βάση $1,\theta,...,\theta^{n-1}$. Έστω τώρα $a_1,...,a_n$ τυχαία βάση του $K$. Γράφοντας

$$a_k = \sum_j b_{kj}\theta^j, \quad b_{kj} \in \mathbb{Q}, \quad k = 1,...,n$$

παίρνουμε από τον ορισμό του γινομένου πινάκων ότι

$$\Delta(a_1,...,a_n) = \det(\sigma_i(a_k))^2 = \det\left(\sum_j b_{kj}\theta_i^j\right)^2$$

$$= \det(b_{kj})^2 \det(\theta_i^j)^2 = \det(b_{kj})^2 \Delta(1,\theta,...,\theta^{n-1}).$$

Ισχύει $\det(b_{kj}) \neq 0$ γιατί ο πίνακας $(b_{kj})$ είναι πίνακας αλλαγής βάσης διανυσματικού χώρου. Επειδή $\Delta(1,\theta,...,\theta^{n-1}) \neq 0$ έχουμε και $\Delta(a_1,...,a_n) \neq 0$. Τέλος $\det(b_{kj})^2$, $\Delta(1,\theta,...,\theta^{n-1}) \in \mathbb{Q}$ και άρα $\Delta(a_1,...,a_n) \in \mathbb{Q}$.

□

**9.2.4 Παρατήρηση** Αν $A = \{a_1,...,a_n\}$ και $A' = \{a_1',...,a_n'\}$ είναι δύο βάσεις του $K$ ως $\mathbb{Q}$ διανυσματικός χώρος και $B$ είναι ο πίνακας μετάβασης από την $A$ στην $A'$, τότε

$$\Delta(a_1',...,a_n') = (\det B)^2 \Delta(a_1,...,a_n),$$

όπως είδαμε στην προηγούμενη απόδειξη.

## 9.3 Αλγεβρικοί Ακέραιοι, Ακέραιες Βάσεις

Ένα στοιχείο $a \in K$ ενός αριθμητικού σώματος ονομάζεται *αλγεβρικός ακέραιος* αν είναι ρίζα ενός μονικού πολυωνύμου που έχει ακέραιους συντελεστές. (Δες και τη § 7.2). Το σύνολο των αλγεβρικών ακεραίων του $K$ είναι υποδακτύλιος του $K$ σύμφωνα με το Πόρισμα 7.2.5 (Οι αλγεβρικοί ακέραιοι του $K$ είναι η ακέραια θήκη του $\mathbb{Z} \subseteq K$). Ο υποδακτύλιος αυτός συμβολίζεται με $\mathcal{O}_K$.

Για παράδειγμα το στοιχείο

$$a = \frac{1}{2} + \frac{1}{2}\sqrt{5} \in \mathbb{Q}(\sqrt{5})$$

είναι αλγεβρικός ακέραιος γιατί είναι ρίζα του πολυωνύμου

$$\left(x-\frac{1}{2}-\frac{1}{2}\sqrt{5}\right)\left(x-\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)=x^2-x-1.$$

**9.3.1 Πρόταση** *Έστω $a\in K$ όπου το K είναι αριθμητικό σώμα. Τότε το a είναι αλγεβρικός ακέραιος αν και μόνο αν $\mathrm{Irr}(a,\mathbb{Q})\in\mathbb{Z}[x]$, δηλαδή οι συντελεστές του $\mathrm{Irr}(a,\mathbb{Q})$ είναι ακέραιοι.*

**Απόδειξη.** Έστω $p(x)=\mathrm{Irr}(a,\mathbb{Q})$. Αν $p(x)\in\mathbb{Z}[x]$ τότε από τον ορισμό έπεται ότι το $a$ είναι αλγεβρικός ακέραιος αφού $p(a)=0$. Αντίστροφα, έστω $a$ αλγεβρικός ακέραιος. Τότε $q(a)=0$ για κάποιο μονικό $q(x)\in\mathbb{Z}[x]$. Θεωρώντας το $q(x)$ στο $\mathbb{Q}[x]$ συμπεραίνουμε ότι το $p(x)$ διαιρεί το $q(x)$. Έχουμε λοιπόν $h(x)\in\mathbb{Q}[x]$ με την ιδιότητα

$$q(x)=p(x)h(x)$$

και όλα τα πολυώνυμα αυτά είναι μονικά. Απαλοίφοντας παρονομαστές, μπορούμε να γράψουμε

$$\alpha\beta q(x)=p_1(x)h_1(x)$$

όπου $\alpha,\beta\in\mathbb{Z}$ και $p_1(x),h_1(x)\in\mathbb{Z}[x]$ είναι πρωταρχικά. Από το λήμμα του Gauss (Λήμμα 1.3.3), το $p_1(x)h_1(x)$ είναι πρωταρχικό. Άρα $\alpha\beta=\pm1$. Έτσι $a=\pm1$, οπότε $p(x)\in\mathbb{Z}[x]$.

□

**9.3.2. Πόρισμα** *Έστω K αριθμητικό σώμα. Τότε*

$$\mathcal{O}_K\cap\mathbb{Q}=\mathbb{Z}.$$

**Απόδειξη.** Ισχύει βέβαια $\mathbb{Z}\subseteq\mathcal{O}_K\cap\mathbb{Q}$ αφού κάθε $a\in\mathbb{Z}$ είναι ρίζα του $x-a\in\mathbb{Z}[x]$. Αντίστροφα, έστω $a\in\mathcal{O}_K\cap\mathbb{Q}$. Τότε $\mathrm{Irr}(a,\mathbb{Q})=x-a$ γιατί $a\in\mathbb{Q}$. Όμως από την Πρόταση 9.3.1, έχουμε $\mathrm{Irr}(a,\mathbb{Q})\in\mathbb{Z}[x]$. Άρα $a\in\mathbb{Z}$. □

Θα αποδείξουμε στη συνέχεια ότι το $\mathcal{O}_K$ ως $\mathbb{Z}$-πρότυπο είναι ελεύθερο τάξης $n=[K:\mathbb{Q}]$. Αυτό θα επιτευχθεί με τη βοήθεια της έννοιας της διακρίνουσας. Ως άμεσο πόρισμα λαμβάνουμε ότι ο δακτύλιος $\mathcal{O}_K$ είναι της Noether. Το γεγονός αυτό οδηγεί στο συμπέρασμα ότι κάθε στοιχείο του $\mathcal{O}_K$

γράφεται ως γινόμενο αναγώγων παραγόντων (αλλά όχι αναγκαστικά κατά μοναδικό τρόπο!).

**9.3.3 Πρόταση** *Έστω* $a_1,...,a_n$ *βάση του* $K$ *ως* $\mathbb{Q}$*-διανυσματικός χώρος. Αν* $a_1...,a_n \in \mathcal{O}_K$, τότε $\Delta(a_1,...,a_n) \in \mathbb{Z}$.

**Απόδειξη.** Γνωρίζουμε από την Πρόταση 9.2.3 ότι $\Delta(a_1,...,a_n) \in \mathbb{Q}$. Αν $a \in \mathcal{O}_K$ και $\sigma : K \to \mathbb{C}$ είναι μονομορφισμός τότε και $\sigma(a) \in \mathcal{O}_K$ : πράγματι, αν $f(a) = 0$ για μονικό $f(x) \in \mathbb{Z}[x]$ τότε $f(\sigma(a)) = \sigma(f(a)) = 0$, και άρα $\sigma(a) \in \mathcal{O}_K$. Τώρα από τον ορισμό της διακρίνουσας συμπεραίνουμε ότι $\Delta(a_1,...,a_n) \in \mathcal{O}_K$ όταν $a_1,...,a_n \in \mathcal{O}_K$. Άρα $\Delta(a_1,...,a_n) \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ σύμφωνα με το Πόρισμα 9.3.2. □

Σύμφωνα με το Θεώρημα 9.1.2 κάθε αριθμητικό σώμα είναι της μορφής $K = \mathbb{Q}(\theta)$. Η επόμενη πρόταση μας πληροφορεί ότι μπορούμε να επιλέξουμε το $\theta$ να είναι αλγεβρικός ακέραιος.

**9.3.4 Πρόταση** *Έστω* $K$ *ένα αριθμητικό σώμα και* $a \in K$. *Τότε υπάρχει* $m \in \mathbb{Z} - \{0\}$ *με την ιδιότητα* $ma \in \mathcal{O}_K$. *Κατά συνέπεια* $K = \mathbb{Q}(\theta)$ *για κάποιο* $\theta \in \mathcal{O}_K$.

**Απόδειξη.** Έστω $a^n + b_{n-1}a^{n-1} + \cdots + b_0 = 0$ με $b_i \in \mathbb{Q}$. Γράφοντας $b_i = c_i / d_i$ με $c_i, d_i \in \mathbb{Z}$ και πολλαπλασιάζοντας την αρχική εξίσωση με $d^n = (d_1 \cdots d_{n-1})^n$ παίρνουμε

$$(da)^n c_{n-1} \frac{d}{d_{n-1}} (da)^{n-1} + c_{n-2} \frac{d^2}{d_{n-2}} (da)^{n-2} + \cdots + c_0 \frac{d^n}{d_0} = 0.$$

Επειδή οι συντελεστές $c_{n-i} \frac{d^i}{d_{n-i}} \in \mathbb{Z}$, έχουμε $da \in \mathcal{O}_K$.

Για το δεύτερο ισχυρισμό της πρότασης, παρατηρούμε ότι $K = \mathbb{Q}(\theta)$ για κάποιο $\theta \in K$ (Θεώρημα 9.1.2). Από τον πρώτο ισχυρισμό έχουμε $m\theta \in \mathcal{O}_K$ για

κάποιο $m \in \mathbb{Z} - \{0\}$. Ισχύει όμως $\mathbb{Q}(\theta) = \mathbb{Q}(m\theta)$, πράγμα που έπεται αμέσως από τους ορισμούς των $\mathbb{Q}(\theta)$ και $\mathbb{Q}(m\theta)$. □

**9.3.5 Θεώρημα** *Έστω K ένα αριθμητικό σώμα βαθμού n. Τότε το $\mathbb{Z}$-πρότυπο $\mathcal{O}_K$ είναι ελεύθερο τάξης n.*

**Απόδειξη.** Από την Πρόταση 9.3.4 έχουμε $K = \mathbb{Q}(\theta)$ για κάποιο $\theta \in \mathcal{O}_K$. Για ένα τέτοιο $\theta$, τα στοιχεία $1, \theta, ..., \theta^{n-1}$ αποτελούν βάση του $K$ ως $\mathbb{Q}$-διανυσματικός χώρος και κάθε $\theta^i$ είναι αλγεβρικός ακέραιος. Τώρα από όλες τις βάσεις $a_1, ..., a_n$ του $K$ ως $\mathbb{Q}$-διανυσματικός χώρος, όπου κάθε $a_i$ είναι αλγεβρικός ακέραιος, επιλέγουμε μια, έστω $\omega_1, ..., \omega_n$, με την ιδιότητα ο θετικός ακέραιος

$$|\Delta(\omega_1, ..., \omega_n)|$$

(Πρόταση 9.3.3) να είναι ελάχιστος. Ισχυριζόμαστε ότι τα $\omega_1, ..., \omega_n$ αποτελούν βάση του $\mathcal{O}_K$ ως $\mathbb{Z}$-πρότυπο. Έστω (για άτοπο) ότι δεν αποτελούν βάση. Αφού τα $\omega_1, ..., \omega_n$ είναι βάση του $K$ ως $\mathbb{Q}$-διανυσματικός χώρος, η προηγούμενη υπόθεση σημαίνει ότι για κάποιο $\omega \in \mathcal{O}_K$ έχουμε

$$\omega = a_1\omega_1 + \cdots + a_n\omega_n$$

για κάποιο $a_i \in \mathbb{Q} - \mathbb{Z}$. Έστω $a_1 \in \mathbb{Q} - \mathbb{Z}$. Γράφουμε $a_1 = a + r$ με $a \in \mathbb{Z}$ και $0 < r < 1$. Εύκολα ελέγχουμε ότι τα στοιχεία

$$\omega - a\omega_1, \omega_2, ..., \omega_n$$

είναι αλγεβρικοί ακέραιοι και αποτελούν βάση του διανυσματικού χώρου $K$. Ο πίνακας μετάβασης από την πρώτη βάση στη δεύτερη είναι

$$B = \begin{bmatrix} a_1 - a & 0 & 0 & \cdots & 0 \\ a_2 & 1 & 0 & \cdots & 0 \\ a_3 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ a_n & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Σύμφωνα με τη Σημείωση 9.2.4 έχουμε

$$\Delta(\omega - a\omega_1, \omega_2, ..., \omega_n) = (\det B)^2 \Delta(\omega_1, \omega_2, ..., \omega_n).$$

Αλλά $(\det B)^2 = (a_1 - a)^2 = r^2 < 1$, και συνεπώς

$$\Delta(\omega - a\omega_1, \omega_2, ..., \omega_n) < \Delta(\omega_1, \omega_2, ..., \omega_n)$$

που είναι άτοπο. □

**9.3.6 Πόρισμα** *Έστω K ένα αριθμητικό σώμα. Τότε ο δακτύλιος $\mathcal{O}_K$ των αλγεβρικών ακεραίων του K είναι δακτύλιος της Noether.*

**Απόδειξη.** Το Θεώρημα 9.3.5 μας πληροφορεί ότι το $\mathbb{Z}$-πρότυπο $\mathcal{O}_K$ είναι πεπερασμένα παραγόμενο. Άρα το $\mathbb{Z}$-πρότυπο $\mathcal{O}_K$ είναι της Noether (Πόρισμα 5.2.3(i)). Συνεπώς κάθε $\mathbb{Z}$-υποπρότυπο του $\mathcal{O}_K$ είναι πεπερασμένα παραγόμενο (Πρόταση 5.1.1). Ειδικά, κάθε ιδεώδες του $\mathcal{O}_K$ είναι πεπερασμένα παραγόμενο. Άρα ο δακτύλιος $\mathcal{O}_K$ είναι της Noether. □

**9.3.7 Πόρισμα** *Έστω K ένα αριθμητικό σώμα. Κάθε μη μηδενικό μη αντιστρέψιμο στοιχείο $a \in \mathcal{O}_K$.*

**Απόδειξη.** Χρησιμοποιώντας το γεγονός ότι ο δακτύλιος $\mathcal{O}_K$ είναι της Noether (Πόρισμα 9.3.6) η απόδειξη είναι ίδια (λέξη προς λέξη!) με την απόδειξη της Πρότασης 1.2.3 και αφήνεται ως άσκηση. (Στην Πρόταση 1.2.3, ο δακτύλιος *R* ήταν δακτύλιος κυρίων ιδεωδών. Αλλά στην απόδειξη χρησιμοποιούμε μόνο το γεγονός ότι κάθε αύξουσα ακολουθία ιδεωδών του *R* είναι τελικά σταθερή).

□

Το Θεώρημα 9.3.5 μας επιτρέπει να δώσουμε τον εξής ορισμό.

**9.3.8 Ορισμός** *Ακέραια βάση ενός αριθμητικού σώματος K λέγεται κάθε βάση του $\mathbb{Z}$-προτύπου $\mathcal{O}_K$.*

Για παράδειγμα, έστω $K = \mathbb{Q}(\sqrt{2})$. Ισχυριζόμαστε ότι $\mathcal{O}_K = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$. Πράγματι, έστω $a \in \mathcal{O}_K - \mathbb{Q}$. Τότε $1 < \deg \mathrm{Irr}(a, \mathbb{Q}) \le [K : \mathbb{Q}] = 2$. Άρα $\deg \mathrm{Irr}(a, \mathbb{Q}) = 2$. Έστω $a = a_0 + a_1\sqrt{2}$, $a_i \in \mathbb{Q}$. Ισχύει $\mathrm{Irr}(a, \mathbb{Q}) = (x - a_0 - a_1\sqrt{2})(x - a_0 + a_1\sqrt{2}) = x^2 - 2a_0 + a_0^2 - 2a_1$ (γιατί;) Άρα (Πρόταση 9.3.1) $2a_0 \in \mathbb{Z}$

και $a_0^2 - 2a_1 \in \mathbb{Z}$. Εύκολα συμπεραίνουμε ότι $a_0 \in \mathbb{Z}$ και $a_1 \in \mathbb{Z}$. Τελικά $\{1, \sqrt{2}\}$ είναι μια ακέραια βάση του $\mathbb{Q}(\sqrt{2})$.

Έστω $\{a_1,...,a_n\}$ και $\{a_1',...,a_n'\}$ δύο ακέραιες βάσεις του αριθμητικού σώματος *K*. Ο πίνακας μετάβασης από την πρώτη βάση στη δεύτερη, έστω *B*, είναι αντιστρέψιμος και έχει στοιχεία ακεραίους αριθμούς. Άρα $\det B = \pm 1$. Τότε η Σημείωση 9.2.4 μας πληροφορεί ότι οι αντίστοιχες διακρίνουσες ταυτίζονται

$$\Delta(a_1,...,a_n) = \Delta(a_1',...,a_n').$$

Έτσι δίνουμε τον εξής ορισμό.

**9.3.9 Ορισμός** *Η διακρίνουσα ενός αριθμητικού σώματος είναι η τιμή* $\Delta(a_1,...,a_n)$, *όπου* $\{a_1,...,a_n\}$ *είναι οποιαδήποτε ακέραια βάση του K.*

Η διακρίνουσα ενός αριθμητικού σώματος είναι ένας μη μηδενικός ακέραιος αριθμός (Πρόταση 9.3.3). Έχει σημαντικότατες εφαρμογές στην Αλγεβρική Θεωρία Αριθμών.

Ένα εύλογο ερώτημα εδώ είναι πως υπολογίζεται η διακρίνουσα αριθμητικού σώματος, η πως προσδιορίζεται μια ακέραια βάση. Μια μερική απάντηση δόθηκε στην απόδειξη του Θεωρήματος 9.3.5. Η επόμενη πρόταση είναι συχνά χρήσιμη σε συγκεκριμένους υπολογισμούς.

**9.3.10 Πρόταση** *Έστω K ένα αριθμητικό σώμα και βάση* $\{a_1,...,a_n\}$ *του K ως* $\mathbb{Q}$*-διανυσματικός χώρος. Αν* $\{a_1,...,a_n\} \subseteq \mathcal{O}_K$ *και η διακρίνουσα* $\Delta(a_1,...,a_n)$ *δεν διαιρείται με το τετράγωνο πρώτου αριθμού, τότε η βάση* $\{a_1,...,a_n\}$ *είναι ακέραια βάση.*

**Απόδειξη.** Θα δείξουμε ότι το σύνολο $\{a_1,...,a_n\}$ είναι βάση του $\mathbb{Z}$-προτύπου $\mathcal{O}_K$. Έστω $\{b_1,...,b_n\}$ βάση του $\mathbb{Z}$-προτύπου $\mathcal{O}_K$ (Θεώρημα 9.3.5). Αν *B* είναι ο πίνακας μετάβασης από τη βάση $\{b_1,...,b_n\}$ του $\mathbb{Q}$-διανυσματικού χώρου *K* στη βάση $\{a_1,...,a_n\}$ του $\mathbb{Q}$-διανυσματικού χώρου *K*, τότε

$$\Delta(a_1,...,a_n) = (\det B)^2 \Delta(b_1,...,b_n)$$

σύμφωνα με τη Σημείωση 9.2.4. Από την υπόθεση και το γεγονός ότι τα στοιχεία του $B$ είναι ακέραιοι, συμπεραίνουμε ότι $\det B = \pm 1$. Άρα η απεικόνιση $\mathbb{Z}$-προτύπων $\mathcal{O}_K \to \mathcal{O}_K$ που ορίζει ο πίνακας $B$ είναι ισομορφισμός. Το σύνολο $\{a_1,...,a_n\}$ είναι η εικόνα της βάσης $\{b_1,...,b_n\}$ του $\mathbb{Z}$-προτύπου $\mathcal{O}_K$. Συνεπώς το $\{a_1,...,a_n\}$ είναι επίσης βάση του $\mathbb{Z}$-προτύπου $\mathcal{O}_K$. □

Για παράδειγμα, έστω $K = \mathbb{Q}(\sqrt{13}) = \{a + b\sqrt{13} \mid a,b \in \mathbb{Q}\}$. Μια βάση του $\mathbb{Q}$-διανυσματικού χώρου $K$ είναι

$$\left\{1, \frac{1}{2} + \frac{1}{2}\sqrt{13}\right\}.$$

Πράγματι, έχουμε $\left\{1, \frac{1}{2} + \frac{1}{2}\sqrt{13}\right\} \subseteq \mathcal{O}_K$, γιατί το $\frac{1}{2} + \frac{1}{2}\sqrt{13}$ είναι ρίζα του πολυωνύμου

$$\left(x - \frac{1}{2} - \frac{1}{2}\sqrt{13}\right)\left(x - \frac{1}{2} + \frac{1}{2}\sqrt{13}\right) = x^2 - x - 6.$$

Η διακρίνουσα της παραπάνω βάσης είναι

$$\Delta\left(1, \frac{1}{2} + \frac{1}{2}\sqrt{13}\right) = \det \begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{13} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{13} \end{vmatrix} = 13,$$

γιατί οι μονομορφισμοί $\mathbb{Q}(\sqrt{13}) \to \mathbb{C}$ είναι δύο

$$\alpha + \beta\sqrt{13} \mapsto \alpha + \beta\sqrt{13}$$
$$\alpha + \beta\sqrt{13} \mapsto \alpha - \beta\sqrt{13}.$$

Εφόσον ο 13 δεν διαιρείται με το τετράγωνο πρώτου αριθμού, η Πρόταση 9.3.10 μας πληροφορεί ότι η $\mathbb{Q}$-βάση του $K$

$$\left\{1, \frac{1}{2} + \frac{1}{2}\sqrt{13}\right\}$$

είναι ακέραια βάση του $\mathcal{O}_K$.

Το προηγούμενο παράδειγμα δείχνει ότι οι ακέραιες βάσεις δεν έχουν πάντα την αναμενόμενη μορφή: το σύνολο

$$\{1, \sqrt{13}\}$$

ενώ είναι $\mathbb{Q}$-βάση του $K=\mathbb{Q}(\sqrt{13})$ και επιπλέον $\{1,\sqrt{13}\}\subseteq\mathcal{O}_K$, *δεν* είναι όμως ακέραια βάση του $\mathcal{O}_K$. Πράγματι, το στοιχείο

$$\frac{1}{2}+\frac{1}{2}\sqrt{13}\in\mathcal{O}_K\,.$$

δεν γράφεται ως $\mathbb{Z}$-γραμμικός συνδυασμός των 1 και $\sqrt{13}$.

## 9.4 Παράδειγμα: Τετραγωνικά σώματα

*Τετραγωνικό σώμα* είναι ένα αριθμητικό σώμα βαθμού 2. Έστω $K$ ένα τετραγωνικό σώμα. Τότε $K=\mathbb{Q}(\theta)$ για κάποιο αλγεβρικό ακέραιο $\theta\in K$ (Πρόταση 9.3.4). Ο βαθμός του πολυωνύμου $\mathrm{Irr}(\theta,\mathbb{Q})$ είναι 2 (Πρόταση 9.1.5). Έστω

$$\mathrm{Irr}(\theta,\mathbb{Q})=x^2+ax+b\,,$$

όπου $a,b\in\mathbb{Z}$ (Πρόταση 9.3.1). Τότε

$$\theta=\frac{-a\pm\sqrt{a^2-4b}}{2}\,.$$

Ισχύει βέβαια $\mathbb{Q}(\theta)=\mathbb{Q}(\sqrt{a^2-4b})$. Γράφουμε $a^2-4b=r^2d$, όπου $r,d\in\mathbb{Z}$ και το $d$ δεν διαιρείται με το τετράγωνο πρώτου βαθμού. Τότε $\mathbb{Q}(\sqrt{a^2-4b})=\mathbb{Q}(r\sqrt{d})=\mathbb{Q}(\sqrt{d})$. *Συμπέρασμα:* κάθε τετραγωνικό σώμα $K$ γράφεται στη μορφή $K=\mathbb{Q}(\sqrt{d})$, όπου $d\in\mathbb{Z}$ δε διαιρείται με το τετράγωνο πρώτου αριθμού.

Θα προσδιορίσουμε στη συνέχεια το δακτύλιο $\mathcal{O}_K$ του τετραγωνικού σώματος $K=\mathbb{Q}(\sqrt{d})$, καθώς και μια ακέραια βάση και τη διακρίνουσα του $K$.

**9.4.1 Θεώρημα** *Έστω $K=\mathbb{Q}(\sqrt{d})$ τετραγωνικό σώμα όπου το $d\in\mathbb{Z}$ δεν διαιρείται με το τετράγωνο πρώτου αριθμού. Τότε*

$$\mathcal{O}_K\begin{cases}\mathbb{Z}[\sqrt{d}\,], & \text{αν} \quad d\not\equiv 1 \bmod 4\\ \mathbb{Z}\left[\dfrac{1}{2}+\dfrac{1}{2}\sqrt{d}\,\right], & \text{αν} \quad d\equiv 1 \bmod 4\,.\end{cases}$$

*Συνεπώς μια ακέραια βάση του K είναι το σύνολο*

$$\{1,d'\}\,,$$

*όπου*

$$d' = \begin{cases} \sqrt{d}, & \text{αν} \quad d \not\equiv 1 \bmod 4 \\ \dfrac{1}{2} + \dfrac{1}{2}\sqrt{d}, & \text{αν} \quad d \equiv 1 \bmod 4 . \end{cases}$$

*Η διακρίνουσα του K είναι*

$$\Delta = \begin{cases} 4d, & \text{αν} \quad d \not\equiv 1 \bmod 4 \\ d, & \text{αν} \quad d \equiv 1 \bmod 4 . \end{cases}$$

**Απόδειξη.** Το σύνολο $\{1, \sqrt{d}\}$ είναι βάση του $K$ ως $\mathbb{Q}$-διανυσματικός χώρος. Έστω $\alpha \in \mathbb{Q}(\sqrt{d})$. Τότε $\alpha = a_0 + a_1\sqrt{d}$ με $a_i \in \mathbb{Q}$. Άρα

$$\alpha = \frac{l + m\sqrt{d}}{n}$$

με $l, m, n \in \mathbb{Z}$, $n > 0$ και μ.κ.δ. $(l, m, n) = 1$. Έστω $\alpha \in \mathcal{O}_K - \mathbb{Q} (= \mathcal{O}_K - \mathbb{Z})$. Τότε

$$\operatorname{Irr}(\alpha, \mathbb{Q}) = \left( x - \frac{l + m\sqrt{d}}{n} \right) \left( x - \frac{l - m\sqrt{d}}{n} \right) = x^2 - \frac{2l}{n} x + \frac{l^2 - m^2 \sqrt{d}}{n^2},$$

γιατί $\deg \operatorname{Irr}(\alpha, \mathbb{Q}) > 1$ (αφού $\alpha \notin \mathbb{Q}$) και το $\operatorname{Irr}(\alpha, \mathbb{Q})$ διαιρεί το πολυώνυμο στο δεξί μέλος (αφού αυτό μηδενίζεται από το $\alpha$). Σύμφωνα με την Πρόταση 9.3.1, έχουμε

$$\frac{2l}{n} \in \mathbb{Z}, \quad \frac{l^2 - m^2 d}{n^2} \in \mathbb{Z} . \qquad (*)$$

Έστω $p$ ένας πρώτος αριθμός που διαιρεί το $l$ και το $n$. Τότε από τη δεύτερη σχέση παίρνουμε $p^2 \mid m^2 d$. Επειδή το $d$ δεν διαιρείται με το τετράγωνο πρώτου αριθμού συμπεραίνουμε ότι $p \mid m$. Αλλά τότε $p \mid$ μ.κ.δ. $(l, m, n) = 1$ που είναι άτοπο. Άρα μ.κ.δ. $(l, n) = 1$. Από την πρώτη σχέση παίρνουμε $n = 1$ ή 2.

Ισχύει $d \not\equiv 1 \bmod 4 \Rightarrow n = 1$.

Πράγματι, αν $n = 2$, τότε μ.κ.δ. $(l, n) = 1 \Rightarrow l$ είναι περιττός. Από τη δεύτερη σχέση των $(*)$ παίρνουμε $m$ περιττός. Συνεπώς $l^2 \equiv m^2 \equiv 1 \bmod 4$. Από τη δεύτερη σχέση των $(*)$ παίρνουμε τότε $d \equiv 1 \bmod 4$, άτοπο.

Ισχύει $d \equiv 1 \bmod 4 \Rightarrow n = 1$ ή 2.

Αυτό έχει ήδη αποδειχθεί (ανεξάρτητα από το $d$).

Από τον πρώτο ισχυρισμό έχουμε $\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt{d}]$ όταν $d \not\equiv 1 \bmod 4$, και από το δεύτερο ισχυρισμό έχουμε $\mathcal{O}_K \subseteq \mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{d}\right]$ όταν $d \equiv 1 \bmod 4$. Επειδή οι αντίστροφες σχέσεις $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$ (για $d \not\equiv 1 \bmod 4$) και $\mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{d}\right] \subseteq \mathcal{O}_K$ (για $d \equiv 1 \bmod 4$) είναι προφανείς, προκύπτουν ισότητες. Μένει να βρούμε τη διακρίνουσα του *K*.

Οι μονομορφισμοί $\mathbb{Q}(\sqrt{d}) \to \mathbb{C}$ είναι δύο

$$a_0 + a_1\sqrt{d} \mapsto a_0 + a_1\sqrt{d}$$
$$a_0 + a_1\sqrt{d} \mapsto a_0 - a_1\sqrt{d}.$$

Συνεπώς η διακρίνουσα $\Delta$ του *K* είναι

$$\Delta = \det\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = 4d, \quad \text{αν} \quad d \not\equiv 1 \bmod 4$$

$$\Delta = \det\begin{pmatrix} 1\frac{1}{2}+\frac{1}{2}\sqrt{d} \\ 1\frac{1}{2}-\frac{1}{2}\sqrt{d} \end{pmatrix}^2 = d, \quad \text{αν} \quad d \equiv 1 \bmod 4,$$

σύμφωνα με τον Ορισμό 9.3.9. □

## 9.5 **Εφαρμογή:** Παραγοντοποίηση σε τετραγωνικά σώματα και Διοφαντικές εξισώσεις.

Είδαμε στο Πόρισμα 9.3.7 ότι για αριθμητικό σώμα *K* κάθε μη μηδενικό μη αντιστρέψιμο στοιχείο του $\mathcal{O}_K$ γράφεται ως γινόμενο αναγώγων στοιχείων. Γνωρίζουμε ότι γενικά η παραγοντοποίηση αυτή δεν είναι μοναδική (Παράδειγμα 1.1.4). Τα παρακάτω θεωρήματα μας παρέχουν παραδείγματα όπου ο $\mathcal{O}_K$ είναι περιοχή μοναδικής παραγοντοποίησης για κάποια τετραγωνικά σώματα *K*.

**9.5.1 Θεώρημα** *Έστω* $K = \mathbb{Q}(\sqrt{d})$ *τετραγωνικό σώμα όπου το d δεν διαιρείται με το τετράγωνο πρώτου βαθμού. Αν* $d < 0$, *τότε ο δακτύλιος* $\mathcal{O}_K$ *είναι Ευκλείδεια περιοχή αν και μόνο αν*

$$d = -1,-2,-3,-7,-11.$$

*Σε καθεμιά από τις περιπτώσεις αυτές, μια Ευκλείδεια συνάρτηση* $\varphi : \mathcal{O}_K - \{0\} \to \mathbb{N}$ *είναι ο περιορισμός της συνάρτησης*

$$\mathbb{Q}(\sqrt{d}) \ni a + b\sqrt{d} \mapsto a^2 - b^2 d \in \mathbb{N}.$$

**9.5.2 Θεώρημα** *Έστω* $K = \mathbb{Q}(\sqrt{d})$ *τετραγωνικό σώμα όπου το d δεν διαιρείται με το τετράγωνο πρώτου αριθμού. Αν* $d > 0$, *τότε ο δακτύλιος* $\mathcal{O}_K$ *είναι Ευκλείδεια περιοχή με Ευκλείδεια συνάρτηση* $\varphi : \mathcal{O}_K - \{0\} \to \mathbb{N}$ *τον περιορισμό της συνάρτησης*

$$\mathbb{Q}(\sqrt{d}) \ni a + b\sqrt{d} \mapsto | a^2 - b^2 d | \in \mathbb{N}$$

*αν και μόνο αν* $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73$.

Το πρώτο θεώρημα χαρακτηρίζει το τετραγωνικό σώμα $K = \mathbb{Q}(\sqrt{d})$ με $d < 0$, όπου ο $\mathcal{O}_K$ είναι Ευκλείδεια περιοχή, ενώ το δεύτερο χαρακτηρίζει τα τετραγωνικά σώματα $K = \mathbb{Q}(\sqrt{d})$ με $d > 0$ όπου ο $\mathcal{O}_K$ είναι Ευκλείδεια περιοχή *ως προς τη δεδομένη συνάρτηση*. Παραμένει ανοικτό το ερώτημα αν ο $\mathcal{O}_K$ για $K = \mathbb{Q}(\sqrt{d})$, $d > 0$, δύναται να είναι Ευκλείδειος ως προς διαφορετική συνάρτηση. Ο Samuel (1971) εικάζει ότι αυτό συμβαίνει για $d = 14$. Η απόδειξη του πρώτου θεωρήματος δεν είναι δύσκολη σε αντίθεση με το δεύτερο θεώρημα που οπωσδήποτε είναι ένα βαθύ αποτέλεσμα. Παραλείπουμε τις αποδείξεις και ερχόμαστε αμέσως σε παραδείγματα Διοφαντικών εξισώσεων που λύνονται με τη βοήθεια της μοναδικής παραγοντοποίησης στους αλγεβρικούς ακεραίους των τετραγωνικών σωμάτων που μνημονεύονται στα παραπάνω θεωρήματα. Πρώτα όμως ας δούμε την έννοια της νόρμας.

Έστω $K = \mathbb{Q}(\sqrt{d})$ τετραγωνικό σώμα. Αν $a = a_0 + a_1\sqrt{d}$, θέτουμε $N(a) = a_0^2 - a_1^2 d$ που ονομάζεται *νόρμα* του *a*. Έτσι ορίζεται μια απεικόνιση $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$. Ισχύει $N(a) = \sigma_1(a)\sigma_2(a)$, όπου $\sigma_1, \sigma_2$ είναι μονομορφισμοί $\mathbb{Q}(\sqrt{d}) \to \mathbb{C}$. Άρα $N(ab) = N(a)N(b)$ για κάθε $a, b \in \mathbb{Q}(\sqrt{d})$. Αν $a \in \mathcal{O}_K$, τότε $N(a) \in \mathbb{Z}$. Πράγματι για $a \in \mathbb{Q}$, οπότε $a \in \mathbb{Z}$ κατά το Πόρισμα 9.3.2, αυτό είναι προφανές, ενώ για $a \notin \mathbb{Q}$ ισχύει $\mathrm{Irr}(a, \mathbb{Q}) = x^2 - 2a_0 x + a_0^2 - a_1^2 d$, οπότε $a_0^2 - a_1^2 d \in \mathbb{Z}$ κατά την Πρόταση 9.3.1.

**9.5.3 Λήμμα** *Τα αντιστρέψιμα στοιχεία του* $\mathbb{Z}[i]$ *είναι* $\{\pm 1, \pm i\}$ *και τα αντιστρέψιμα στοιχεία του* $\mathbb{Z}[\sqrt{2}]$ *είναι* $\{\pm 1\}$.

**Απόδειξη.** Έστω $a, b \in \mathbb{Z}[\sqrt{-2}]$ με $ab = 1$. Τότε $N(ab) = N(1) = 1$ οπότε $N(a)N(b) = 1$. Άρα $N(a) = \pm 1$. Γράφοντας $a = a_0 + a_1\sqrt{-2}$, $a_i \in \mathbb{Z}$ έχουμε $a_0^2 + 2a_1^2 = \pm 1$. Οι μόνες λύσεις είναι $(a_0, a_1) = (\pm 1, 0)$. Η απόδειξη για το $\mathbb{Z}[i]$ είναι παρόμοια (ή δες την Πρόταση 1.5.4). □

**9.5.4 Παράδειγμα** Η Διοφαντική εξίσωση $x^3 = y^2 + 2$ έχει ακριβώς δύο λύσεις $x = 3$, $y = \pm 5$.

**Απόδειξη.** Θεωρούμε το τετραγωνικό σώμα $K = \mathbb{Q}(\sqrt{-2})$. Τότε $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$ σύμφωνα με την Πρόταση 9.4.1. Ο δακτύλιος $\mathcal{O}_K$ είναι Ευκλείδεια περιοχή σύμφωνα με το Θεώρημα 9.5.1 και συνεπώς περιοχή μοναδικής παραγοντοποίησης (Πρόταση 1.5.2 και Θεώρημα 1.2.1). Έστω τώρα $x^3 = y^2 + 2$. Παραγοντοποιούμε στο $\mathcal{O}_K$,

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2}). \tag{6}$$

Έστω $a + b\sqrt{-2} \in \mathcal{O}_K$ κοινός διαιρέτης των $y + \sqrt{-2}$ και $y - \sqrt{-2}$. Τότε αυτός διαιρεί το άθροισμα, δηλαδή

$$a + b\sqrt{-2} \mid 2y$$

και τη διαφορά, δηλαδή

$$a + b\sqrt{-2} \mid 2\sqrt{-2}.$$

Χρησιμοποιώντας τη νόρμα, οι δύο τελευταίες σχέσεις δίνουν

$$a^2 + 2b^2 \mid 4y^2 \quad \text{και} \quad a^2 + 2b^2 \mid 8.$$

Επειδή ο $y$ είναι περιττός ($y$ άρτιος $\Rightarrow x^3 = y^2 + 2$ είναι άρτιος $\Rightarrow x$ άρτιος $\Rightarrow 8 \mid y^2 + 2$ άτοπο) λαμβάνουμε

$$a^2 + 2b^2 \mid 4$$

και άρα $a^2 + 2b^2 = 1, 2, 4$. Οι μόνες λύσεις είναι βέβαια

$$(a,b) = (\pm 1,0), (0,\pm 1), (\pm 2,0)$$

οπότε

$$a + b\sqrt{-2} = \pm 1, \pm\sqrt{-2}, \pm 2 .$$

Ισχυριζόμαστε ότι $a + b\sqrt{-2} = \pm 1$. Πρώτα, αν $a + b\sqrt{-2} = \pm\sqrt{-2}$ τότε από τη σχέση $a + b\sqrt{-2} \mid y + \sqrt{-2}$ παίρνουμε $\sqrt{-2} \mid y$, δηλαδή $y$ άρτιος που είναι άτοπο. Με παρόμοιο τρόπο αποκλείεται η δεύτερη περίπτωση $a + b\sqrt{-2} = \pm 2$. Συνεπώς $a + b\sqrt{-2} = \pm 1$, δηλαδή οι μόνοι κοινοί διαιρέτες των $y + \sqrt{-2}$ και $y - \sqrt{-2}$ είναι οι $\pm 1$. Χρησιμοποιώντας τώρα το γεγονός ότι η παραγοντοποίηση στο $\mathcal{O}_K$ είναι μοναδική και τη σχέση (6) συμπεραίνουμε ότι

$$y + \sqrt{-2} = \pm(c + d\sqrt{-2})^3 \tag{7}$$

για κάποιο $c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, γιατί το $y + \sqrt{-2}$ είναι μη μηδενικό μη αντιστρέψιμο στοιχείο του $\mathbb{Z}[\sqrt{-2}]$ σύμφωνα με το Λήμμα 9.5.3. Οι συντελεστές του $\sqrt{-2}$ στην (7) δίνουν

$$1 = \pm d(3c^2 - 2d^2) .$$

Η τελευταία εξίσωση έχει ακριβώς τις λύσεις $c = \pm 1$, $d = \pm 1$. Τότε παίρνουμε $x = 3$, $y = \pm 5$ από τις (7) και (6). □

**9.5.5 Παράδειγμα** Η Διοφαντική εξίσωση

$$x^3 = y^2 + 4$$

έχει ακριβώς τέσσερις λύσεις: $x = 5$, $y = \pm 1$ και $x = 2$, $y = \pm 2$.

**Απόδειξη.** 1η περίπτωση: $y$ είναι περιττός. Εργαζόμενοι στο δακτύλιο $\mathbb{Z}[i]$, που είναι περιοχή μοναδικής παραγοντοποίησης, έχουμε

$$x^3 = (2 + iy)(2 - iy) . \tag{8}$$

Έστω $a + bi$ ένας κοινός διαιρέτης των $2 + iy$ και $2 - iy$. Όπως ακριβώς στο προηγούμενο παράδειγμα καταλήγουμε στο συμπέρασμα ότι κάθε κοινός διαιρέτης των $2 + iy$ και $2 - iy$ είναι $\pm 1, \pm i$ (που είναι αντιστρέψιμα στοιχεία). Άρα από την (8) και τη μοναδικότητα της παραγοντοποίησης παίρνουμε

$$2 + iy = \varepsilon(a + ib)^3$$

όπου $a+ib\in\mathbb{Z}[i]$ και $\varepsilon$ είναι μονάδα. Αλλά $\varepsilon=\pm1,\pm i$ (Λήμμα 9.5.3) και καθένα απ' αυτά είναι τρίτη δύναμη στο $\mathbb{Z}[i]$. Άρα

$$2+iy=(a+ib)^3 \tag{9}$$

για κάποιο $a+ib\in\mathbb{Z}[i]$. Παίρνοντας συζυγή στοιχεία (ή και εφαρμόζοντας τον μονομορφισμό $\sigma_2:\mathbb{Q}(i)\to\mathbb{C}$, $a+ib\mapsto a-ib$) έχουμε

$$2-iy=(a-ib)^3. \tag{10}$$

Προσθέτοντας τις (9) και (10) και εκτελώντας τις πράξεις έχουμε

$$2=a(a^2-3b^2).$$

Οι λύσεις είναι $a=-1$, $b=\pm1$ και $a=2$, $b=\pm1$. Τότε η (8) δίνει

$$x^3=((a+ib)(a-ib))^3=(a^2+b^2)^3$$

οπότε για τις δύο λύσεις έχουμε $x=2$ και $x=5$. Φυσικά $y^2+4=2^3$, $5^3\Rightarrow y=\pm2,\pm11$. Όμως το $y$ είναι περιττός. Άρα $x=5$, $y=\pm11$.

$2^{\eta}$ περίπτωση: $y$ άρτιος. Τότε και ο $x$ είναι άρτιος. Γράφοντας $x=2x_0$, $y=2y_0$ παίρνουμε

$$2x_0^3=y_0^2+1=(y_0+i)(y_0-i)=(1+iy_0)(1-iy_0). \tag{10}$$

Ισχυριζόμαστε ότι μ.κ.δ.$(y_0+i,y_0-i)=1+i$. Κάθε κοινός διαιρέτης των $y_0+i$ και $y_0-i$ θα διαιρεί τη διαφορά τους $2i$, ενώ ισχύει $2i=(1+i)^2$. Άρα μ.κ.δ.$(y_0+i,y_0-i)=1$, $1+i$, $(1+i)^2$ γιατί το $1+i$ είναι ανάγωγο στοιχείο του $\mathbb{Z}[i]$ ($N(1+i)=2=$πρώτος αριθμός· Άσκηση 6). Όμως το $1+i$ διαιρεί τα $y_0+i$ και $y_0-i$ γιατί

$$y_0\pm i=\left(\frac{y_0+1}{2}\pm i\frac{1-y_0}{2}\right)(1+i)$$

και $\frac{y_0+1}{2},\frac{1-y_0}{2}\in\mathbb{Z}$. Επιπλέον το $(1+i)^2$ δεν διαιρεί το $y_0+i$ σε διαφορετική περίπτωση το $1+i$ θα διαιρούσε το $\frac{y_0+1}{2}+i\frac{1-y_0}{2}$. Όμως η σχέση

$$\frac{y_0+1}{2}+i\frac{1-y_0}{2}=(1+i)(a+ib)$$

δίνει $2a = 1$. Άρα πράγματι μ.κ.δ.$(y_0 + i, y_0 - i) = 1 + i$. Τώρα από τη σχέση $2x^3 = (1 + iy_0)(1.iy_0)$, δηλαδή τη σχέση

$$(1+i)^2 x^3 = (1+iy_0)(1-iy_0)$$

και τη μοναδικότητα της παραγοντοποίησης συμπεραίνουμε ότι

$$1 + iy_0 = (1+i)(a+ib)^3 \tag{12}$$

για κάποιο $a + ib \in \mathbb{Z}[i]$. Τα πραγματικά μέρη στην παραπάνω σχέση είναι

$$1 = (a+b)(a^2 - 4ab + b^2).$$

Οι λύσεις είναι $a = \pm 1$, $b = 0$ και $a = 0$, $b = \pm 1$. Αλλά τότε $y = -2$ από τη (12). Άρα $x = 2$ από την (11). □

Οι διοφαντικές εξισώσεις των προηγούμενων παραδειγμάτων οφείλονται στον Fermat.

## Ασκήσεις

**1.** Βρείτε ένα $\theta$ έτσι ώστε $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\theta)$.

**2.** Ποιοι είναι οι μονομορφισμοί $\mathbb{Q}(\sqrt[4]{3}) \to \mathbb{C}$; Ποια είναι τα πολυώνυμα $\mathrm{Irr}(\sqrt[4]{3}, \mathbb{Q})$, $\mathrm{Irr}(\sqrt{3}, \mathbb{Q})$;

**3.** Έστω $\theta$ ρίζα του $x^2 - 2x + 5$ στο $\mathbb{C}$. Ποιος είναι ο δακτύλιος $\mathcal{O}_K$, όπου $K = \mathbb{Q}(\theta)$. Ποια είναι η διακρίνουσα του $K$;

**4.** Έστω $\theta$ ρίζα του $x^2 - 2x + 6$ στο $\mathbb{C}$. Βρείτε μια ακέραια βάση και τη διακρίνουσα του $K = \mathbb{Q}(\theta)$.

**5.** Έστω $K = \mathbb{Q}(\sqrt{d})$, όπου $d < 0$ και δεν διαιρείται από το τετράγωνο πρώτου αριθμού. Αν $d < -3$ αποδείξετε ότι τα αντιστρέψιμα στοιχεία του $\mathcal{O}_K$ είναι $\{\pm 1\}$. Για $d = -3$ υπάρχουν 6 αντιστρέψιμα στοιχεία $\{\pm 1, \pm\omega, \pm\omega^2\}$, όπου $\omega^3 = 1$ και $\omega \neq 1$.

**6.** Έστω $K$ τετραγωνικό σώμα και $a \in \mathcal{O}_K$. Αν $N(a)$ είναι πρώτος αριθμός, τότε το $a$ είναι ανάγωγο στο $\mathcal{O}_K$. Είναι το στοιχείο $3+2\sqrt{-2}$ ανάγωγο στο $\mathbb{Q}(\sqrt{-2})$; Το 3 στο $\mathbb{Z}[i]$; Ισχύει το αντίστροφο του πρώτου ισχυρισμού;

**7.** Ποια είναι η παραγοντοποίηση του 13 σε γινόμενο αναγώγων στοιχείων του $\mathcal{O}_K$ όπου $K=\mathbb{Q}(\sqrt{-3})$; (Υπόδειξη: Άσκηση 6).

**8.** Αποδείξετε ότι ο δακτύλιος $\mathbb{Z}(\sqrt{10})$ δεν είναι περιοχή μοναδικής παραγοντοποίησης (Υπόδειξη: $2\cdot 3 = (4+\sqrt{10})(4-\sqrt{10})$).

**9.** Στο $\mathbb{Z}[i]$ ισχύει $10=(3+i)(3-i)=2\cdot 5$, ενώ ο $\mathbb{Z}[i]$ είναι περιοχή μοναδικής παραγοντοποίησης. Εξηγήστε.

**10.** Το πλήθος των αντιστρέψιμων στοιχείων του $\mathcal{O}_K$ όπου $K=\mathbb{Q}(\sqrt{3})$, είναι πεπερασμένο;

**11.** Έστω $\zeta$ ρίζα στο $\mathbb{C}$ του $x^2+x+1$. Αποδείξετε ότι $\{1,\zeta,\zeta^2\}$ είναι μια ακέραια βάση του $K=\mathbb{Q}(\zeta)$ και κατά συνέπεια $\mathcal{O}_K=\mathbb{Z}[\zeta]$. Ποια είναι η διακρίνουσα του $K$;

**12.** (Μια εικασία του Ramanugan που αποδείχθηκε από τον Nagell). Οι λύσεις της Διοφαντικής εξίσωσης

$$x^2+7=2^n$$

είναι οι παρακάτω

$$(x,n)=(\pm 1,3),(\pm 3,4),(5,5),(\pm 11,7),(\pm 181,5).$$

Υπόδειξη: $1^{\text{ο}}$ βήμα. Για $n$ άρτιο έχουμε $7=(2^{n/2}+x)(2^{n/2}-x)$ οπότε $(x,n)=(3,4)$.

$2^{\text{ο}}$ βήμα. Έστω $n>3$ περιττός. Θέτοντας $m=n-2$ έχουμε

$$\frac{x^2+7}{4}=2^m$$

οπότε μια παραγοντοποίηση είναι

$$\frac{x+\sqrt{-7}}{2}\,\frac{x-\sqrt{-7}}{2}=\left(\frac{x+\sqrt{-7}}{2}\right)^m\left(\frac{x-\sqrt{-7}}{2}\right)^m.$$

Από τη μοναδικότητα της παραγοντοποίησης στο $\mathcal{O}_K$ όπου $K = \mathbb{Q}(\sqrt{-7})$ (Θεώρημα 9.5.1) και την Άσκηση 5 παίρνουμε

$$\frac{x \pm \sqrt{-7}}{2} = \pm\left(\frac{1+\sqrt{-7}}{2}\right)^m$$

και άρα

$$\pm\sqrt{-7} = \left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1-\sqrt{-7}}{2}\right)^m .$$

$3^o$ βήμα. Στην παραπάνω σχέση μόνο το πρόσημο – στο αριστερό σκέλος ισχύει.

$4^o$ βήμα. Ισχύει $-2^{m-1} \equiv m \bmod 7$. Αφού $2^6 \equiv 1 \bmod 7$ παίρνουμε $m \equiv 3, 5, 13 \bmod 42$.

$5^o$ βήμα. $m = 3, 5, 13$.

**13.** Ποιες είναι οι λύσεις της Διοφαντικής εξίσωσης $y^2 + 1 = x^3$;

**14.** Έστω *k* αριθμητικό σώμα. Πότε ο δακτύλιος $\mathcal{O}_K$ είναι του Artin;

# Κεφάλαιο 10

# Τοπικοποίηση

Θα ασχοληθούμε εδώ με μια στοιχειώδη αλλά σημαντική γενίκευση της κατασκευής του σώματος πηλίκων ακεραίας περιοχής $R$. Εδώ ο $R$ επιτρέπεται να έχει μηδενοδιαιρέτες. Για πολλαπλασιαστικό υποσύνολο $S$ του $R$ θα μελετήσουμε τα πρώτα ιδεώδη του $S^{-1}R$. Η τοπικοποίηση είναι μια θεμελιώδης τεχνική που ανάγει προβλήματα της Μεταθετικής Άλγεβρας στην περίπτωση των τοπικών δακτυλίων.

## 10.1 Ρητές Καμπύλες

Είδαμε στην Πρόταση 0.7.1 μια τεχνική με την οποία κατασκευάζεται το σώμα πηλίκων μια ακεραίας περιοχής $R$: στο σύνολο $R\times S$, όπου $S = R - \{0\}$, ορίσαμε κατάλληλη σχέση ισοδυναμίας. Θα δούμε εδώ ότι η τεχνική αυτή γενικεύεται στις περιπτώσεις που ο $R$ έχει μηδενοδιαιρέτες και το $S$ είναι οποιοδήποτε πολλαπλασιαστικό υποσύνολο του $R$. Ο νέος δακτύλιος $S^{-1}R$, είναι δυνατό να έχει μηδενοδιαιρέτες. Για κατάλληλη εκλογή του $S$ θα οδηγηθούμε στη σημαντικότατη έννοια της τοπικοποίησης.

Έστω $R$ ένας δακτύλιος και $S \subseteq R$ ένα πολλαπλασιαστικό υποσύνολο του $R$. Υπενθυμίζουμε ότι αυτό σημαίνει: $1 \in S$ και αν $s, s' \in S$ τότε $ss' \in S$. Στο $R\times S$ ορίζουμε μια σχέση ισοδυναμίας

$$(r,s) \sim (r',s') \Leftrightarrow \text{ υπάρχει } u \in S \text{ με την ιδιότητα } u(rs' - r's) = 0.$$

Είναι θέμα ρουτίνας να δείξουμε ότι η σχέση ~ είναι πράγματι σχέση ισοδυναμίας. Η κλάση ισοδυναμίας που περιέχει το στοιχείο $(r,s)$ θα συμβολίζεται με $r/s$. Το σύνολο των κλάσεων ισοδυναμίας συμβολίζεται με $S^{-1}R$. Δηλαδή

$$S^{-1}R = \left\{ \frac{r}{s} \mid r \in R,\ s \in S \right\}.$$

Στο $S^{-1}R$ ορίζουμε τις πράξεις

$$\frac{r}{s} + \frac{r'}{s'} = \frac{r\,s' + r'\,s}{s\,s'}$$

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{r\,r'}{s\,s'}.$$

Ως προς τις πράξεις αυτές το $S^{-1}R$ είναι μεταθετικός δακτύλιος· το μηδενικό στοιχείο είναι $0/1$ και το μοναδιαίο είναι το $1/1$. Η επαλήθευση των αξιωμάτων είναι υπόθεση ρουτίνας. Ενδεικτικά ας επαληθεύουμε ότι η πρόσθεση είναι καλά ορισμένη.

Έστω $\frac{r}{s} = \frac{\bar{r}}{\bar{s}}$ και $\frac{r'}{s'} = \frac{\bar{r}'}{\bar{s}'}$. Τότε υπάρχουν $u, v \in S$ με τις ιδιότητες

$$u(r\,\bar{s} - \bar{r}\,s) = v(r'\,\bar{s}' - \bar{r}'\,s') = 0.$$

Επομένως παίρνουμε

$$u\,v\,(r\,\bar{s}\,s'\,\bar{s}' - \bar{r}\,s\,s'\,\bar{s}') = 0$$

$$u\,v\,(r'\,\bar{s}'\,s\,\bar{s} - \bar{r}'\,s'\,s\,\bar{s}) = 0$$

Προσθέτοντας τις παραπάνω εξισώσεις παίρνουμε

$$u\,v(\bar{s}\,\bar{s}'(r\,s' + r'\,s) - s\,s'(\bar{r}\,\bar{s}' + \bar{r}'\,\bar{s})).$$

Άρα

$$\frac{r\,s' + r'\,s}{s\,s'} = \frac{\bar{r}\,\bar{s}' + \bar{r}'\,\bar{s}}{\bar{s}\,\bar{s}'}.$$

**10.1.1 Σημείωση** 1) Αν $S = R - \{0\}$, όπου $R$ είναι ακέραια περιοχή, τότε ο δακτύλιος $S^{-1}R$ είναι το σώμα πηλίκων του $R$. Πράγματι, από τη σχέση $u(r\,s' - r'\,s) = 0$ του ορισμού παίρνουμε $r\,s' - r'\,s = 0$, γιατί $u \neq 0$. Τώρα δες την απόδειξη της πρότασης 0.7.1.

2) Στο $S^{-1}R$ ισχύει $\frac{r}{s} = 0 = \frac{0}{1} \Leftrightarrow$ υπάρχει $u \in S$ με την ιδιότητα $u(r1 - 0s) = 0$, δηλαδή $ur = 0$.

3) Η απεικόνιση $f : R \ni r \mapsto \frac{r}{1} \in S^{-1}R$ είναι ομομορφισμός δακτυλίων, αλλά όχι αναγκαστικά μονομορφισμός (όπως ήταν στην Πρόταση 0.7.1). Για παράδειγμα έστω $R = \mathbb{Z}_{10}$ και $S = \{[1],[5]\}$. Τότε $[2] \in \ker f$ σύμφωνα με την προηγούμενη σημείωση. Η απεικόνιση $f : R \to S^{-1}R$ ονομάζεται *φυσικός ομομορφισμός*.

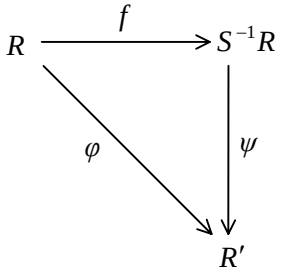
**10.1.2 Παράδειγμα** Έστω $R = \mathbb{Z}, t \in \mathbb{Z}$ και $S = \{1, t, t^2, \ldots\}$. Τότε

$$S^{-1}R = \left\{ \frac{r}{t^k} \in \mathbb{Q} \,\middle|\, k \in N \right\}.$$

Ο παραπάνω δακτύλιος συμβολίζεται με $\mathbb{Z}_t$ και δεν πρέπει να συγχέεται με τον δακτύλιο πηλίκο $\mathbb{Z}/(t)$. Ο τελευταίος θα συμβολίζεται με $\mathbb{Z}/t\mathbb{Z}$.

Ποιο γενικά, αν $t \in R$ και $S = \{1, t, t^2, \ldots\}$ θα συμβολίζουμε το δακτύλιο $S^{-1}R$ με $R_t$.

**10.1.3 Πρόταση** *Έστω $\phi : R \to R'$ ένας ομομορφισμός δακτυλίων και $S \subseteq R$ ένα πολλαπλαστιαστικό σύνολο. Αν για κάθε $s \in S$ το $\varphi(s)$ είναι αντιστρέψιμο τότε υπάρχει μοναδικός ομομορφισμός δακτυλίων $\psi : S^{-1}R \to R'$ που καθιστά το διάγραμμα*




*μεταθετικό, όπου f είναι ο φυσικός ομομορφισμός.*

**Απόδειξη** i) Ύπαρξη. Ορίζουμε $\psi : S^{-1}R \to R'$

$$\varphi\left(\frac{r}{s}\right) = \varphi(r)\varphi(s)^{-1} \qquad (r \in R,\ s \in S)$$

Αρκεί να δείξουμε ότι η απεικόνιση $\psi$ είναι καλά ορισμένη, γιατί τότε θα είναι προφανώς ομομορφορισμός δακτυλίων που ικανοποιεί τη ζητούμενη συνθήκη. Έστω

$$\frac{r_1}{s_1} = \frac{r_2}{s_2}$$

Τότε υπάρχει $u \in S$ έτσι ώστε

$$u(r_1 s_2 - r_2 s_1) = 0$$

Εφαρμόζοντας τον $\varphi$ παίρνουμε

$$\varphi(u)\,(\varphi(r_1)\varphi(s_2) - \varphi(r_2)\varphi(s_1)) = 0\,.$$

Το $\varphi(u)$ είναι αντιστρέψιμο. Άρα $\varphi(r_1)\varphi(s_2) - \varphi(r_2)\varphi(s_1) = 0$, δηλαδή $\varphi(r_1)\varphi(s_1)^{-1} = \varphi(r_2)\varphi(s_2)^{-1}$, δηλαδή $\psi\left(\frac{r_1}{s_1}\right) = \psi\left(\frac{r_2}{s_2}\right)$.

ii) Μοναδικότητα. Έστω $\psi : S^{-1}R \to R'$ ομομορφισμός δακτυλίων που καθιστά το διάγραμμα μεταθετικό. Θα δείξουμε ότι $\psi\left(\frac{r}{s}\right) = \varphi(r)\varphi(s)^{-1}$ για κάθε $r \in R,\ s \in S$ πράγμα που αμέσως δίνει τη μοναδικότητα του $\psi$. Έχουμε λόγω της μεταθετικότητας

$$\psi\left(\frac{r}{1}\right) = \psi f(r) = \varphi(r)$$

για κάθε $r \in R$. Τώρα αν $s \in S$ έχουμε

$$\psi\left(\frac{1}{s}\right) = \psi\left(\left(\frac{s}{1}\right)^{-1}\right) = \psi\left(\frac{s}{1}\right)^{-1} = \varphi(s)^{-1}$$

λόγω της προηγούμενης ισότητας. Τελικά

$$\psi\left(\frac{r}{s}\right) = \psi\left(\frac{r}{1}\right)\psi\left(\frac{1}{s}\right)^{-1} = \varphi(r)\varphi(s)^{-1}\,. \qquad \square$$

Ως πόρισμα λαμβάνουμε μια πρόταση που είναι συχνά χρήσιμη στον προσδιορισμό του $S^{-1}R$. Πρώτα όμως παρατηρούμε ότι ο φυσικός ομομορφισμός $f : R \to S^{-1}R$ έχει τις ακόλουθες ιδιότητες:

1) $s \in S \Rightarrow f(s)$ είναι αντιστρέψιμο στον $S^{-1}R$.

Πράγματι, $\frac{s}{1}\frac{1}{s}=\frac{1}{1}$

2) $r \in \ker f \Rightarrow rs = 0$ για κάποιο $s \in S$.

Βλέπε σημείωση 10.1.1 (2).

3) Κάθε στοιχείο του $S^{-1}R$ έχει τη μορφή $f(r)\, f(s)^{-1}$ για κάποιο $r \in R.$ και $s \in S$.

Πράγματι, $\frac{r}{s}=\frac{r}{1}\frac{1}{s}=\frac{r}{1}\left(\frac{s}{1}\right)^{-1}$.

Το επόμενο πόρισμα μας πληροφορεί ότι οι παραπάνω τρεις συνθήκες προσδιορίζουν τον $S^{-1}R$ μονοσήμαντα (με προσέγγιση ισομορφισμού εννοείται).

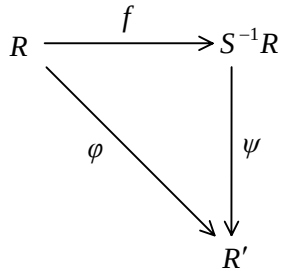
**10.1.4 Πόρισμα** *Έστω $\phi : R \to R'$ ομομορφισμός δακτυλίων και $S \subseteq R$ πολλαπλαστιαστικό σύνολο. Αν ο φ ικανοποιεί τις συνθήκες*

*1) $s \in S \Rightarrow \phi(s)$ αντιστρέψιμο στον R΄.*

*2) $r \in Kerf \Rightarrow rs = 0$ για κάποιο $s \in S$.*

*3) κάθε στοιχείο του R΄ έχει τη μορφή $\phi(r)\, \phi(s)^{-1}$ για κάποια $r \in R$, $s \in S$*

*τότε υπάρχει μοναδικός ισομορφισμός $\psi : S^{-1}R \to R'$ που καθιστά μεταθετικό το διάγραμμα*




*όπου f είναι ο φυσικός ισομορφισμός.*

**Απόδειξη** Υπάρχει μοναδικός ομομορφισμός $\psi$ που καθιστά το παραπάνω διάγραμμα μεταθετικό λόγω της συνθήκης 1) και της Πρότασης 10.1.3. Επιπλέον ισχύει $\psi\left(\frac{r}{s}\right)=\varphi(r)\,\varphi(s)^{-1}$ όπως είδαμε στην απόδειξη της Πρότασης 10.1.3. Τώρα

η συνθήκη 3) μας πληροφορεί ότι ο $\psi$ είναι επιμορφισμός. Έστω $\frac{r}{s} \in \ker\psi$. Τότε $\varphi(r)=0$. Από τη συνθήκη 2) παίρνουμε $r\,s'=0$ για κάποιο $s' \in S$. Αλλά τότε $\frac{r}{s}=\frac{0}{1}$ στο $S^{-1}R$. Συνεπώς ο $\psi$ είναι και μονομορφισμός. □

**10.1.5 Παράδειγμα** Με τη βοήθεια του προηγούμενου Πορίσματος θα δείξουμε ότι αν $t \in R$ και $S=\{1,t,t^2,\ldots\}$ τότε $S^{-1}R \cong \frac{R[x]}{(tx-1)}$.

**Απόδειξη** Θεωρούμε τον ομομορφισμό δακτυλίων

$$\varphi : R \ni r \mapsto r+(tx-1) \in \frac{R[r]}{(tx-1)}.$$

1) Το αντίστροφο του $\varphi(t^n)=t^n+(tx-1)$ είναι το $x^n+(tx-1)$, γιατί $t^n x^n-1=(tx-1)(t^{n-1}x^{n-1}+t^{n-2}x^{n-2}+\cdots+1)$.

2) Αν $r \in \ker\varphi$ τότε $r+(tx-1)=(tx-1)$, οπότε $r=g(x)(tx-1)$ για κάποιο $g(x) \in R[x]$. Γράφουμε $g(x)=g_m x^m+g_{m-1}x^{m-1}+\cdots+g_0$ και εξισώνουμε συντελεστές. Παίρνουμε

$$\begin{aligned} 0&=g_m t\\ 0&=g_{m-1}t+gm\\ &\cdots\cdots\cdots\cdots\\ 0&=g_0 t+g_1\\ r&=g_0 \end{aligned}$$

Πολλαπλασιάζοντας τη δεύτερη εξίσωση με $t$ και αφαιρώντας από την πρώτη παίρνουμε $g_{m-1}t^2=0$. Συνεχίζοντας με αυτόν τον τρόπο λαμβάνουμε τελικά $rt^{m-1}=0$. Έτσι $rs=0$ για κάποια $s \in S$, που είναι το ζητούμενο.

3) Έστω $g(x)+(tx-1) \in \frac{R[x]}{(tx-1)}$, όπου $g(x) \in R[x]$. Γράφοντας $g(x)=g_m x^m+\cdots+g_0$ και για συντομία $I=(tx-1)$ έχουμε $x+1=(t+I)^{-1}$ από το 1). Άρα εργαζόμενοι στο πηλίκο $\frac{R[x]}{I}$ έχουμε

$$\begin{aligned} g(x)+I &= g_m(x+I)^m + \cdots + g_1(x+I) + g_0 + I \\ &= g_m(x+I)^{-m} + \cdots + g_1(x+I)^{-1} + g_0 + I \\ &= (g_m + g_{m-1}(t+I) + \cdots + g_1(t+I)^{m-1} + g_0(t+I)^m + I)(t+I)^{-1} \\ &= ((g_m + g_{m-1}t + \cdots + g_1 t^{m-1} + g_0 t^m) + I)(t+I)^{-m} \\ &= ((g_m + g_{m-1}t + \cdots + g_1 t^{m-1} + g_0 t^m) + I)(t^m + I)^{-1}. \end{aligned}$$

Θέτοντας $r = g_m + g_{m-1}t + \cdots + g_1 t^{m-1} + g_0 t^m$ και $s = t^m$ έχουμε τότε

$$g(x) + I = \varphi(r)\varphi(s)^{-1}$$

πράγμα που επαληθεύει την τρίτη συνθήκη. Τελικά, το πόρισμα 10.1.4 δίνει τον ισομορφισμό $S^{-1}R \cong \dfrac{R[x]}{(tx-1)}$. □

## 10.2 Ιδεώδη του $S^{-1}R$

Θα μελετήσουμε εδώ τη μορφή των ιδεωδών του $S^{-1}R$ σε σχέση με τα ιδεώδη του *R*. Ειδικότερα θα περιγράψουμε τα πρώτα ιδεώδη του $S^{-1}R$ συναρτήσει των πρώτων ιδεωδών του *R*. Θα χρειαστούμε πρώτα κάποιες γενικότητες.

Έστω λοιπόν $f : R \to R'$ ένας ομομορφισμός δακτυλίων. Αν $J$ είναι ιδεώδες του *R'*, υπενθυμίζουμε ότι το σύνολο

$$f^{-1}(J) = \{r \in R \mid f(r) \in J\}$$

είναι ιδεώδες του *R*. Το $f^{-1}(J)$ ονομάζεται *συστολή* του *J* στο *R* και συμβολίζεται με $J^c$ (όταν εννοείται ποιον ομομορφισμό $f$ έχουμε θεωρήσει). Αν *I* είναι ιδεώδες του *R* τότε το σύνολο

$$f(I)R' = \left\{\sum f(a_i)r_i' \mid a_i \in I,\ r_i' \in R\right\}$$

είναι ιδεώδες του *R'*, το ιδεώδες του *R'* που παράγεται από την εικόνα $f(I)$. Συμβολίζεται συχνά με $I^e$ και ονομάζεται επέκταση του $I$ στο *R'*. Η απόδειξη του επόμενου λήμματος έπεται άμεσα από τους διαφόρους ορισμούς και αφήνεται ως άσκηση. Ο συμβολισμός $I^{ec}$ σημαίνει $(I^e)^c$.

**10.2.1 Λήμμα** Έστω $I, I_1, I_2$ ιδεώδη του $R$. Έστω $J, J_1, J_2$ ιδεώδη του $R'$ και $f : R \to R'$ ένας ομομορφισμός δακτυλίων. Τότε

1) $(I_1 + I_2)^e = I_1^e + I_2^e$

2) $(I_1 I_2)^e = I_1^e I_2^e$

3) $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$

4) $(\sqrt{J})^c = \sqrt{J^c}$

5) $I \subseteq I^{ec}$

6) $J^{ce} \subseteq J$

7) $I^e \subseteq I^{ece}$

8) $J^c \subseteq J^{cec}$.

Συμβολίζουμε το σύνολο των ιδεωδών ενός δακτυλίου $R$ με $I_R$. Αν $f : R \to R'$ είναι ένας ομομορφισμός δακτυλίων, θεωρούμε δύο άλλα σύνολα ιδεωδών (τις συστολές και τις επεκτάσεις)

$$C_R = \{J^c \mid J \in I_{R'}\} \subseteq I_R$$

$$E_{R'} = \{I^e \mid I \in I_R\} \subseteq I_R \qquad \square$$

**10.2.2 Πόρισμα** *Οι απεικονίσεις*

$$C_R \to E_{R'} \quad E_{R'} \to C_R$$
$$I \mapsto I^e \qquad J \mapsto J^c$$

*είναι αντίστροφες και συνεπώς 1-1 αντιστοιχίες.*

**Απόδειξη** Λήμμα 10.2.1 7) και 8). $\square$

Ερχόμαστε τώρα στη συγκεκριμένη περίπτωση που μας ενδιαφέρει: $S \subseteq R$ είναι πολλαπλασιαστικό υποσύνολο του δακτυλίου $R$ και $f : R \to S^{-1}R'$, $f(r) = r/1$, είναι ο φυσικός ομομορφισμός.

**10.2.3 Λήμμα** *Ισχύει* $I_{S^{-1}R} = E_{S^{-1}R}$, *δηλαδή κάθε ιδεώδες του* $S^{-1}R$ *είναι η επέκταση κάποιου ιδεώδους του R.*

**Απόδειξη** Έστω $J$ ένα ιδεώδες του $S^{-1}R$. Θα δείξουμε ότι

$$J = J^{ce}$$

οπότε βέβαια $J \in E_{S^{-1}R}$. Έστω $a \in J$. Τότε $a = r/s$ για κάποια $r \in R$ και $s \in S$. Έχουμε $r \in J^c$ γιατί

$$f(r) = \frac{r}{1} = \frac{s}{1}\frac{r}{s} \in J .$$

Τώρα

$$a = \frac{r}{s} = \frac{1}{s}\frac{r}{1} = \frac{1}{s} f(r) \in J^{ce}$$

Άρα $J \subseteq J^{ce}$. Η άλλη σχέση $J \subseteq J^{ce}$ είναι το λήμμα 10.2.1 6). □

Μας ενδιαφέρουν λοιπόν οι επεκτάσεις ιδεωδών του $R$.

**10.2.4 Λήμμα** *Έστω $I$ ένα ιδεώδες του $R$. Τότε*

$$I^e = \left\{ a \in S^{-1}R \mid a = \frac{r}{s} \quad \text{για κάποια} \quad r \in I,\ s \in S \right\}.$$

**Απόδειξη** "$\supseteq$" Έχουμε (όπως και πριν) $a = \frac{r}{s} = \frac{r}{1}\frac{1}{s} = f(r)\frac{1}{s}$ και άρα $a \in I^e$.

"$\subseteq$". Το τυχαίο στοιχείο του $I^e$ έχει τη μορφή $b = \sum f(a_i) r_i^{'}$ όπου $a_i \in I$ και $r_i^{'} \in S^{-1}R$. Γράφοντας $r_i^{'} = r_i / s_i$, αντικαθιστώντας στην προηγούμενη εξίσωση και γράφοντας τα κλάσματα με κοινό παρανομαστή προκύπτει ότι $b = r/s$, όπου $r \in R$ και $s\left(= \prod s_i\right) \in S$.

□

**10.2.5 Πόρισμα** *Αν ο $R$ είναι δακτύλιος της Noether τότε και ο $S^{-1}R$ είναι δακτύλιος της Noether.*

**Απόδειξη** Από το Λήμμα 10.2.3 κάθε ιδεώδες $S^{-1}R$ έχει τη μορφή $I^e$, όπου $I$ ιδεώδες του $R$. Το $I$ είναι πεπερασμένα παραγόμενο, $I = (a_1, \ldots, a_n)$. Από το Λήμμα 10.2.4, το $I^e$ παράγεται από τα στοιχεία $\frac{a_1}{1}, \ldots, \frac{a_n}{1}$, και άρα είναι

πεπερασμένα παραγόμενο.

□

Σύμφωνα με το Λήμμα 10.2.4 κάθε στοιχείο $a \in I^e$ έχει μια τουλάχιστον παράσταση της μορφής $a = r/s$ με $r \in R$ και $s \in S$. *Δεν* αληθεύει ότι αν $a = r/s$ με $r \in R$ και $s \in S$, τότε $r \in I$ (Άσκηση 1). Αν όμως το $I$ είναι πρώτο ιδεώδες και $(I \cap S = \varnothing)$ τότε το παρακάτω λήμμα μας πληροφορεί ότι όντως $r \in I$.

**10.2.6 Λήμμα** *Έστω $P$ ένα πρώτο ιδεώδες του $R$ με $P \cap S = \varnothing$. Έστω $a = \frac{r}{s} \in P^e$ με $r \in R$ και $s \in S$.* Τότε *$r \in P$. Επιπλέον ισχύει $P^{ec} = P$.*

**Απόδειξη** Αφού $\frac{r}{s} \in P^e$ *έχουμε* $\frac{r}{s} = \frac{r_1}{s_1}$ με $r_1 \in P$ και $s_1 \in S$ (Λήμμα 10.2.4). Άρα $u(r s_1 - r_1 s) = 0$ για κάποιο $u \in S$. Συνεπώς $urs_1 = ur_1 s \in P$. Αλλά $us_1 \in S$. Άρα $us_1 \notin P$ γιατί $P \cap S = \varnothing$. Αφού $urs_1 \notin P$ και το $P$ είναι πρώτο ιδεώδες παίρνουμε $r \in P$. Για τον τελευταίο ισχυρισμό του Λήμματος πρώτα παρατηρούμε ότι $P \subseteq P^{ec}$ (Λήμμα 10.2.1 5). Έστω $a \in P^{ec}$. Τότε $\left(\frac{a}{1}\right) \in P^e$. Από το πρώτο μέρος του λήμματος έχουμε $a \in P$. Άρα $P^{ec} = P$.

□

**10.2.7 Θεώρημα** *Έστω $S \subseteq R$ ένα πολλαπλασιαστικό υποσύνολο του δακτυλίου $R$.*

*(i) Αν P είναι ένα πρώτο ιδεώδες του R και $P \cap S = \varnothing$, τότε το $P^e$ είναι πρώτο ιδεώδες του $S^{-1}R$.*

*(ii) Αν $P'$ είναι πρώτο ιδεώδες του $S^{-1}R$, τότε το $(P')^c$ είναι πρώτο ιδεώδες του R και $(P')^c \cap S = \varnothing$.*

*Κατά συνέπεια κάθε πρώτο ιδεώδες του $S^{-1}R$ είναι της μορφής $P^e$ για μοναδικό πρώτο ιδεώδες P του R με την ιδιότητα $P \cap S = \varnothing$.*

**Απόδειξη** (i) Ισχύει $P^e \subsetneq S^{-1}R$, γιατί αν $P^e = S^{-1}R$ τότε $P^{ec} = (S^{-1}R)^c = R$, οπότε σύμφωνα με το λΛήμμα 10.2.6 θα είχαμε $P = R$ που είναι άτοπο, αφού το $P$ είναι πρώτο ιδεώδες του $R$. Έστω $a = \frac{r}{s} \in S^{-1}R$ και $a' = \frac{r'}{s'} \in S^{-1}R$ με $aa' = P^e$. Τότε από τη σχέση $\frac{rr'}{ss'} \in P$ και το Λήμμα 10.2.6 παίρνουμε $rr' \in P$. Άρα $r \in P$ ή $r' \in P$, γιατί το $P$ είναι πρώτο. Συνεπώς $\frac{r}{s} \in P^e$ ή $\frac{r'}{s'} \in P^e$, δηλαδή το $P^e$ είναι πρώτο.

(ii) Το $(P')^c$ είναι πρώτο γιατί γενικά η συστολή πρώτου ιδεώδους είναι πρώτο (Άσκηση 2). Από το λΛήμμα 10.2.3 έχουμε $P' = I^e$ για κάποιο ιδεώδες $I$ του $R$. Από το Λήμμα 10.2.1 7) συμπεραίνουμε τότε ότι $(P')^{ec} = P'$. Η τελευταία σχέση σημαίνει ότι $(P')^c \cap S = \varnothing$, γιατί διαφορετικά θα είχαμε

$$s \in (P')^c \cap S \Rightarrow \frac{1}{1} = \frac{s}{s} \in (P')^{ec} = P' \Rightarrow P' = R.$$

Για τον τελευταίο ισχυρισμό του θεωρήματος, έστω $P'$ πρώτο ιδεώδες του $S^{-1}R$. Τότε $P' = P^e$ για κάποιο ιδεώδες $P$ του $R$ (Λήμμα 10.2.3) και το $P$ είναι το πρώτο (μέρος i) του θεωρήματος). Ισχύει $P \cap S = \varnothing$, γιατί $P \subseteq P^{ec}$ (Λήμμα 10.2.1 5)) και $P^{ec} \cap S = \varnothing$ (μέρος ii) του θεωρήματος). Τέλος αν $P$ και $Q$ είναι πρώτα ιδεώδη του $R$ με $P^e = Q^e$ και $P \cap S = Q \cap S = \varnothing$, τότε $P^{ec} = Q^{ec}$ οπότε το Λήμμα 10.2.6 δίνει $P = Q$.

□

Ας συμβολίσουμε το σύνολο των πρώτων ιδεωδών του δακτυλίου $R$ με $\mathrm{Spec}(R)$. Το προηγούμενο θεώρημα μας πληροφορεί ότι η αντιστοιχία

$$\{P \in \mathrm{Spec}\, R \mid P \cap S = \varnothing\} \ni P \to P^e \in \mathrm{Spec}(S^{-1}R)$$

είναι 1-1 με αντίστροφη την

$$\mathrm{Spec}(S^{-1}R) \ni P' \to (P')^c \in \{P \in \mathrm{Spec}\, R \mid P \cap S = \varnothing\}.$$

Έστω $R$ δακτύλιος και $P$ πρώτο ιδεώδες του $R$. Τότε το σύνολο $S = R - P$ είναι πολλαπλασιαστικό υποσύνολο του $R$. Ο δακτύλιος $S^{-1}R$ ονομάζεται *τοπικοποίηση*

του $R$ στο $P$ και συμβολίζεται με το $R_P$. Το Θεώρημα 10.2.7 μας πληροφορεί ότι ο $R_P$ είναι τοπικός δακτύλιος: Ισχύει $\{Q \in \operatorname{Spec} R \mid Q \cap S \neq \varnothing\} = Q \in \operatorname{Spec} R \mid Q \subseteq P\}$ γιατί $S = R - P$. Τώρα η αντιστοιχία ιδεωδών παίρνει τη μορφή

$$\{Q \in \operatorname{Spec} R \mid Q \subseteq P\} \ni Q \mapsto Q^e \in \operatorname{Spec} R_P$$

Έστω $\underline{m}$ μέγιστο ιδεώδες του $R_P$. Τότε το $\underline{m}$ είναι μέγιστο στοιχείο του συνόλου $\operatorname{Spec} R_P$. Επειδή η αντιστοιχία διατηρεί τις σχέσεις υποσυνόλου έχουμε ότι το $\underline{m}^c$ είναι μέγιστο στοιχείο του συνόλου $\{Q \in \operatorname{Spec} R \mid Q \subseteq P\}$. Αλλά το σύνολο αυτό έχει προφανώς μοναδικό μέγιστο στοιχείο το $P$. Άρα ο δακτύλιος $R_P$ έχει μοναδικό μέγιστο ιδεώδες το

$$P^e = \{\frac{a}{b} \mid a \in P,\ b \in R - P\}$$

(Λήμμα 10.2.4). Έτσι αποδείξαμε την πρόταση.

**10.2.9 Πρόταση** *Έστω $P$ ένα πρώτο ιδεώδες του $R$. Τότε ο δακτύλιος $R_P$ είναι τοπικός με μέγιστο ιδεώδες το*

$$P^e = \left\{\frac{a}{b} \mid a \in P, b \in R - P\right\}.$$

Για παράδειγμα, έστω $p$ πρώτος αριθμός. Τότε

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z},\ p \ \text{ δεν διαιρεί το } \ b\right\}$$

και το μέγιστο ιδεώδες είναι

$$\left\{\frac{pa}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z},\ p \ \text{ δεν διαιρεί το } \ b\right\}.$$

Έστω $k$ σώμα και $R = k[x]$. Έστω $P = (x - a)$, όπου $a \in k$. Τότε

$$k[x]_{(x-a)} = \left\{\frac{f}{g} \in k(x) \middle| \ f,\ g \in k[x],\ g(a) \neq 0\right\}$$

και το μέγιστο ιδεώδες είναι

$$\left\{\frac{(x-a)f}{g} \in k(x) \middle| \ f,\ g \in k[x],\ g(a) \neq 0\right\}.$$

Η Πρόταση 10.2.9 μπορεί να αποδειχθεί άμεσα χωρίς τη χρήση του θεωρήματος 10.2.8 (Άσκηση 3).

## 10.3 Πρότυπα Πηλίκων

Γενικεύουμε εδώ την κατασκευή του δακτυλίου πηλίκων $S^{-1}R$ στην περίπτωση που το $R$ αντικαθίσταται από $R$-πρότυπο $M$. Θα είμαστε σύντομοι όπου οι τεχνικές είναι παρόμοιες με αυτές της Παραγράφου 10.1.

Έστω λοιπόν $S \subseteq R$ πολλαπλασιαστικό υποσύνολο του δακτυλίου $R$ και $M$ ένα $R-$πρότυπο. Στο σύνολο $M \times S$ ορίζουμε μια σχέση ισοδυναμίας

$$(m,s) \sim (m',s') \Leftrightarrow \exists t \in S \quad \text{με την ιδιότητα} \quad t(sm' - s'm) = 0 .$$

Η κλάση ισοδυναμίας που περιέχει το στοιχείο $(m,s)$ συμβολίζεται με $m/s$. Το σύνολο των κλάσεων ισοδυναμίας συμβολίζεται με

$$S^{-1}M = \left\{ \frac{m}{s} \middle| \; m \in M, s \in R \right\}.$$

Με τις πράξεις

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$$

$$r\frac{m}{s} = \frac{rm}{s}$$

το σύνολο $S^{-1}M$ αποκτά τη δομή $R$-προτύπου.

Αν $f : M \to N$ είναι ομομορφισμός $R$-προτύπων τότε η απεικόνιση

$$S^{-1}f : S^{-1}M \ni \frac{m}{s} \mapsto \frac{f(m)}{s} \in S^{-1}N$$

είναι ομομορφισμός $S^{-1}$ $R$ – προτύπων. Αν $g : L \to M$ είναι δεύτερος ομομορφισμός $R$-προτύπων, τότε $S^{-1}(f \circ g) = S^{-1}(f) \circ S^{-1}(g)$.

**Σημείωση** Οι αποδείξεις ότι η σχέση ~ είναι σχέση ισοδυναμίας, ότι οι πράξεις $S^{-1}M$ είναι καλά ορισμένες, ότι το $S^{-1}M$ είναι $R$-πρότυπο, ότι η $S^{-1}(f)$ είναι καλά ορισμένη, κλπ. είναι απλό θέμα ρουτίνας και παραλείπονται.

Μια χρήσιμη πρόταση είναι η ακόλουθη.

**10.3.1 Πρόταση** *Έστω $S \subseteq R$ πολλαπλασιαστικό υποσύνολο του δακτυλίου $R$ και*

$$L \xrightarrow{f} M \xrightarrow{g} N$$

*ακριβής ακολουθία R-προτύπων. Τότε η ακολουθία* $S^{-1}R$ *προτύπων*

$$S^{-1}L \xrightarrow{S^{-1}(f)} S^{-1}M \xrightarrow{S^{-1}(g)} S^{-1}N$$

*είναι επίσης ακριβής.*

**Απόδειξη**. Ισχύει $\ker g = \operatorname{Im} f$ και θα αποδείξουμε ότι $\ker S^{-1}(g) = \operatorname{Im} S^{-1}(f)$. Αρχικά παρατηρούμε ότι $\operatorname{Im} S^{-1}(f) \subseteq \ker S^{-1}(g)$ γιατί $S^{-1}(f) \circ S^{-1}(g) = S^{-1}(f \circ g) = S^{-1}(0) = 0$. Έστω τώρα $\frac{m}{s} \in \ker S^{-1}(g)$. Τότε $\frac{g(m)}{s} = 0$. Άρα υπάρχει $t \in S$ με την ιδιότητα $tg(m) = 0$. Συνεπώς $g(tm) = 0$. Άρα $tm \in \ker g = \operatorname{Im} f$. Δηλαδή $tm = f(\ell)$ για κάποιο $\ell \in L$. Τώρα $\frac{m}{s} = \frac{f(\ell)}{st} = S^{-1}(f)\left(\frac{\ell}{st}\right) \in \operatorname{Im} S^{-1}(f)$. Άρα $\ker S^{-1}(g) \subseteq \operatorname{Im} S^{-1}(f)$. □

Αν το $L$ είναι υποπρότυπο του $M$, είναι η προηγούμενη πρόταση επιτρέπει να θεωρήσουμε το $S^{-1}L$ ως $S^{-1}R$ υποπρότυπο του $S^{-1}M$, γιατί η απεικόνιση $S^{-1}L \to S^{-1}M, \frac{\ell}{s} \mapsto \frac{\ell}{s}$ είναι μονομορφισμός. Έχοντας υπόψη αυτήν την παρατήρηση λαμβάνουμε το εξής πόρισμα.

**10.3.2 Πόρισμα** *Έστω L, N υποπρότυπα του M. Τότε*

*(i)* $S^{-1}(L+N) = S^{-1}(L) + S^{-1}(N)$

*(ii)* $S^{-1}(L \cap N) = S^{-1}(L) \cap S^{-1}(N)$

*(iii) υπάρχει ισομορφισμός* $S^{-1}R$ *- προτύπων* $S^{-1}(M/N) \cong S^{-1}(M)/S^{-1}(N)$

**Απόδειξη.** (i) Προκύπτει αμέσως από την ταυτότητα $\frac{\ell + n}{s} = \frac{\ell}{s} + \frac{n}{s}$.

(ii) Η σχέση $S^{-1}(L \cap N) = S^{-1}(L) \cap S^{-1}(N)$ προκύπτει άμεσα από τους ορισμούς. Έστω τώρα $a \in S^{-1}(L) \cap S^{-1}(N)$. Τότε υπάρχουν $\ell \in L, n \in N, t \in S$ με

την ιδιότητα $a = \frac{\ell}{s} = \frac{n}{t}$. Τότε $u(t\ell - sn) = 0$ για κάποιο $u \in S$. Όμως $ut\ell = usn \in L \cap N$. Θέτοντας $b = ut\ell$ έχουμε $\frac{\ell}{s} = \frac{b}{stu} \in S^{-1}(L \cap N)$. Άρα $S^{-1}(L) \cap S^{-1}(N) \subseteq S^{-1}(L \cap N)$.

(iii) Από την ακριβή ακολουθία

$$0 \to N \to M \to M/N \to 0$$

η Πρόταση 10.3.1 δίνει την ακριβή ακολουθία

$$0 \to S^{-1}N \to S^{-1}M \to S^{-1}M/N \to 0 .$$

Από την τελευταία προκύπτει το ζητούμενο. □

Αν $P$ είναι πρώτο ιδεώδες και $S = R - P$ το $S^{-1}M$ θα συμβολίζεται με $M_P$. Αν $S^{-1}R = R_P$ -πρότυπο. Το $M_P$ ονομάζεται *τοπικοποίηση* του $M$ στο $P$. Αν $f : M \to N$ είναι ομομορφισμός $R$-προτύπων και $P$ πρώτο ιδεώδες του $R$, ο ομομορφισμός $S^{-1}(f) : M_P \to N_P$, όπου $S = R - P$, θα συμβολίζεται με $f_P$.

Μια ιδιότητα $Q$ του $R$-προτύπου $M$ ονομάζεται *τοπική* αν παρακάτω συνθήκες είναι ισοδύναμες:

(i) το $M$ έχει την ιδιότητα $Q$

(ii) το $M_P$ έχει την ιδιότητα $Q$ για κάθε πρώτο ιδεώδες $P$.

Ακολουθούν δύο απλά παραδείγματα τοπικών ιδιοτήτων. Για δύο άλλα παραδείγματα δες τις ασκήσεις 5 και 10, ενώ για ένα αντιπαράδειγμα δες την Άσκηση 12.

**10.3.3 Πρόταση** *Έστω $R$-πρότυπο $M$. Τα ακόλουθα είναι ισοδύναμα*

*(i)* $M = 0$

*(ii)* $M_P = 0$ *για κάθε πρώτο ιδεώδες* $P$ *του* $R$

*(iii)* $M_{\underline{m}} = 0$ *για κάθε μέγιστο ιδεώδες* $\underline{m}$ *του* $R$.

**Απόδειξη.** (i) $\Rightarrow$ (ii). Προφανές

(ii) $\Rightarrow$ (iii). Προφανές γιατί κάθε μέγιστο ιδεώδες είναι πρώτο.

(iii)$\Rightarrow$(i). Έστω ότι ισχύει $M_{\underline{m}} = 0$ για κάθε μέγιστο ιδεώδες $\underline{m}$. Αν $M \neq 0$, τότε υπάρχει $a \in M, a \neq 0$. Θεωρούμε το ιδεώδες $I = \text{ann}(a)$. Αφού $I \neq R$ (γιατί $1a = a \neq 0$), το $I$ περιέχεται σε μέγιστο ιδεώδες, $I \subseteq \underline{m}$, σύμφωνα με το Πόρισμα 3.5.3. Επειδή $M_{\underline{m}} = 0$ έχουμε $a/1 = 0$. Άρα υπάρχει $s \in S = R - \underline{m}$ με την ιδιότητα $sa = 0$. Όμως τότε $s \in \text{ann}(a) \subseteq m$, που είναι άτοπο. □

**10.3.4 Πρόταση** *Έστω $f : M \to N$ ένας ομομορφισμός R-προτύπων. Τα ακόλουθα είναι ισοδύναμα*

*(i) $o\, f$ είναι μονομορφισμός*

*(ii) $o\ f_p : M_P \to N_P$ είναι μονομορφισμός για κάθε πρώτο ιδεώδες $P$ του $R$*

*(iii) $o\ f_{\underline{m}} : M_{\underline{m}} \to N_{\underline{m}}$ είναι μονομορφισμός για κάθε μέγιστο ιδεώδες $\underline{m}$ του R.*

**Απόδειξη.** (i)$\Rightarrow$(ii). Από την ακριβή ακολουθία $0 \to M \to N$, η Πρόταση 10.2.1 δίνει την ακριβή ακολουθία $0 \to M_P \to N_P$.

(ii)$\Rightarrow$(iii). Προφανές γιατί κάθε μέγιστο ιδεώδες είναι πρώτο.

(iii)$\Rightarrow$(ii). Έστω $L = \ker f$. Από την ακριβή ακολουθία

$$0 \to L \to M \xrightarrow{f} N$$

παίρνουμε την ακριβή ακολουθία (Πρόταση 10.3.1)

$$0 \to L_{\underline{m}} \to M_{\underline{m}} \xrightarrow{f_{\underline{m}}} N_{\underline{m}}$$

για κάθε μέγιστο ιδεώδες $\underline{m}$ του $R$. Από την υπόθεση παίρνουμε $L_{\underline{m}} = 0$. Από την Πρόταση 10.3.3 iii) έχουμε $L = 0$. □

## Ασκήσεις

**1.** Δώστε ένα παράδειγμα όπου $(r/s) \in I^e$ αλλά $r \notin I$ όπως μνημονεύουμε πριν το Λήμμα 10.2.6. (Υπόδειξη: $R \in \mathbb{Z}, S = \{1,3,3^2,\ldots\}, I = (6)$).

**2.** Έστω $f : R \to R'$ ομομορφισμός δακτυλίων. Αν $P$ είναι πρώτο ιδεώδες του $R'$ τότε η συστολή $P^c = f^{-1}(P)$ είναι πρώτο ιδεώδες του $R$.

**3.** Έστω $P$ πρώτο ιδεώδες του $R$. Τότε κάθε στοιχείο $a \in R_P - PR_P$, όπου $PR_P = \left\{ \frac{a}{b} \middle| \ a \in P, b \in R - P \right\}$, είναι αντιστρέψιμα και άρα $R_P$ είναι τοπικός δακτύλιος (Πρόταση 10.2.9).

**4.** Αν το $M$ είναι $R$-πρότυπο του Artin τότε και το $S^{-1}R$ είναι $S^{-1}R$ πρότυπο του Artin.

**5.** Έστω $f : M \to N$ ομομορφισμός $R$-προτύπων. Η ιδιότητα "ο $f$ είναι επιμορφισμός" είναι τοπική.

**6.** Αν το $M$ είναι $R$-πρότυπο ορίζουμε

$$\mathrm{Supp}(M) = \{P \in \mathrm{Spec}\, R \big| M_P \neq 0\} \quad .$$

Έστω $0 \to L \to M \to N \to 0$ ακριβής ακολουθία $R-$προτύπων.

Τότε

$$\mathrm{Supp}(M) = \mathrm{Supp}(L) \cup \mathrm{Supp}(N) \, .$$

**7.** Έστω $I$ ιδεώδες του $R$. Τότε

$$S^{-1}(\sqrt{I}) = \sqrt{S^{-1}(I)}$$

**8.** Έστω $R$ δακτύλιος έτσι ώστε ο $R_P$ δεν έχει μη μηδενικά μηδενοδύναμα στοιχεία για κάθε πρώτο ιδεώδες $P$. Τότε και ο $R$ δεν έχει μη μηδενικά μηδενοδύναμα στοιχεία.

**9.** Έστω $S,T$ πολλαπλασιαστικά υποσύνολα του δακτυλίου $R$. Με $U$ συμβολίζουμε την εικόνα του $T$ στο $S^{-1}R$. Αποδείξτε ότι οι δακτύλιοι $(ST)^{-1}R$ και $U^{-1}(S^{-1}R)$ είναι ισόμορφοι.

**10.** Έστω $R$ ακέραια περιοχή. Τα ακόλουθα είναι ισοδύναμα

(i) $R$ ακέραια κανονική

(ii) $R_p$ είναι κανονική για κάθε πρώτο ιδεώδες $P$ του $R$.

(iii) $R_{\underline{m}}$ είναι κανονική για κάθε μέγιστο ιδεώδες $\underline{m}$ του $R$.

(Μια περιοχή λέγεται κανονική αν είναι ακέραια κλειστή στο σώμα πηλίκων του).

**11.** Έστω $R = \mathbb{Z}/6\mathbb{Z}$ και $S = \{1,3,5\} \subseteq \mathbb{Z}/6\mathbb{Z}$. Τότε $S^{-1}R \cong \mathbb{Z}/2\mathbb{Z}$.

**12.** Αν $R_p$ είναι ακέραια περιοχή για κάθε $P \in \operatorname{Spec} R$ έπεται ότι ο $R$ είναι ακέραια περιοχή;

# Κεφάλαιο 11

# Πρωταρχική Ανάλυση

Σε μια περιοχή μοναδικής παραγοντοποίησης, η ανάγωγη παραγοντοποίηση ενός στοιχείου $\alpha = p_1^{n_1} \cdots p_k^{n_k}$ δίνει για τα αντίστοιχα ιδεώδη $(\alpha) = (p_1)^{n_1} \cap \cdots \cap (p_k)^{n_k}$. Τα ιδεώδη $(p_i)^{n_i}$ δεν είναι πρώτα αλλά έχον την ιδιότητα $bc \in (p)^n \Rightarrow b \in (p)^n$ ή $c^m \in (p)^n$ για κάποιο *m*. Τέτοια ιδεώδη ονομάζονται πρωταρχικά, και η παραπάνω παράσταση του $(a)$ ως τομή πεπερασμένου πλήθους πρωταρχικών ιδεωδών ονομάζεται πρωταρχική ανάλυση του $(a)$. Στο κεφάλαιο αυτό θα μελετήσουμε πρωταρχικές αναλύσεις ιδεωδών σε δακτύλιους της Noether. Θα ασχοληθούμε με το πρόβλημα της ύπαρξης πρωταρχικής ανάλυσης και των μορφών της μοναδικότητας τους. Τέλος ως εφαρμογή θα αναφερθούμε στο θεώρημα τομής του Krull.

Στα παρακάτω με *R* συμβολίζουμε τυχαίο (μεταθετικό) δακτύλιο όχι αναγκαστικά της Noether.

## 11.1 Πρωταρχική Ανάλυση

Θυμίζουμε από την § 6.3 ότι ένα γνήσιο ιδεώδες *Q* του δακτυλίου *R* λέγεται πρωταρχικό αν $xy \in Q \Rightarrow x \in Q$ ή $y^n \in Q$ για κάποιο $n \in \mathbb{N}$. Επιπλέον το ριζικό $P = \sqrt{Q}$ ενός πρωταρχικού ιδεώδες *Q* είναι πρώτο ιδεώδες (Πρόταση 6.3.2). Θα λέμε τότε ότι το *Q* είναι *P – πρωταρχικό*.

Έστω *Q* ένα *P*-πρωταρχικό ιδεώδες. Αν $P'$ είναι πρώτο ιδεώδες με $Q \subseteq P'$ τότε $P = \sqrt{Q} \subseteq \sqrt{P'} = P'$. Συνεπώς το *P* είναι το ελάχιστο πρώτο ιδεώδες που περιέχει το *Q*.

**11.1.1 Ορισμός** *Έστω I ένα γνήσιο ιδεώδες του R. Μια πρωταρχική ανάλυση του I είναι μια παράσταση της μορφής*

$$I = Q_1 \cap \cdots \cap Q_n ,$$

*όπου κάθε ιδεώδες $Q_i$ είναι πρωταρχικό. Το I λέγεται αναλύσιμο αν έχει μια τουλάχιστον πρωταρχική ανάλυση.*

Για παράδειγμα, το ιδεώδες $(x^2 y)$ του $k[x, y]$, όπου $k$ σώμα, είναι αναλύσιμο γιατί μια πρωταρχική ανάλυσή του είναι $(x^2 y) = (x^2) \cap (y)$. Το $(x^2, y)$ είναι αναλύσιμο, γιατί είναι πρωταρχικό, αφού το ριζικό του είναι μέγιστο ιδεώδες, $\sqrt{(x^2, y)} = (x, y)$, σύμφωνα με την άσκηση 6.8. Ισχύει $\sqrt{(x^2, y)} = (x, y)$ γιατί το $(x, y)$ είναι μέγιστο ιδεώδες που περιέχεται στο γνήσιο ιδεώδες $\sqrt{(x^2, y)}$. (Θα δούμε παρακάτω ότι κάθε γνήσιο ιδεώδες δακτυλίου της Noether –και συνεπώς $k[x, y]$– είναι αναλύσιμο!).

**11.1.2 Ορισμός** *Έστω I ένα αναλύσιμο ιδεώδες του R και*

$$I = Q_1 \cap \cdots \cap Q_n$$

*μια πρωταρχική ανάλυση του I. Θέτουμε $P_i = \sqrt{Q_i}$. Η προηγούμενη πρωταρχική ανάλυση λέγεται ελάχιστη πρωταρχική ανάλυση αν*

*1) $P_i \neq P_i$ για κάθε $i \neq j$, και*

*2) για κάθε j ισχύει $I \neq \bigcap_{i \neq j} Q_i$.*

Για παράδειγμα, μια ελάχιστη πρωταρχική ανάλυση του ιδεώδους $(x^2, xy)$ του $k[x, y]$, όπου $k$ σώμα, είναι

$$(x^2, xy) = (x) \cap (x, y)^2 .$$

Υπάρχει όμως και άλλη (!)

$$(x^2, xy) = (x) \cap (x^2, y) .$$

Η πρωταρχική ανάλυση

$$(x^2, xy) = (x) \cap (x, y)^2 \cap (x^2, y)$$

δεν είναι ελάχιστη.

Το παρακάτω λήμμα μας πληροφορεί ουσιαστικά ότι κάθε αναλύσιμο ιδεώδες έχει μια τουλάχιστον ελάχιστη πρωταρχική ανάλυση.

**11.1.3 Λήμμα** *Έστω $P$ ένα πρώτο ιδεώδες του $R$ και $Q_1,\ldots,Q_n$ $P$-πρωταρχικά ιδεώδη. Τότε το ιδεώδες $Q_1 \cap \cdots \cap Q_n$ είναι επίσης $P$-πρωταρχικό.*

**Απόδειξη.** Προφανώς $Q_1 \cap \cdots \cap Q_n \neq R$ αφού $Q \neq R$. Έστω $a,b \in R$ με

$$ab \in Q_1 \cap \cdots \cap Q_n \text{ και } a \notin Q_1 \cap \cdots \cap Q_n .$$

Τότε $a \notin Q_i$ για κάποιο $i$. Αλλά $ab \in Q_1 \Rightarrow b \in \sqrt{Q_i}$ από τον ορισμό του πρωταρχικού ιδεώδους. Άρα $b \in P = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_n} = \sqrt{Q_1 \cap \cdots \cap Q_n}$ (Άσκηση 6.1 ii)). □

Έστω $I$ ένα αναλύσιμο ιδεώδες και

$$I = Q_1 \cap \cdots \cap Q_n \tag{1}$$

μια πρωταρχική ανάλυση του $I$. Έστω $P_i = \sqrt{Q_i}$. Αν για παράδειγμα $P_1 = P_2$ τότε με τη χρήση του Λήμματος 11.1.3 παίρνουμε την πρωταρχική ανάλυση (θέτοντας $Q_2' = Q_1 \cap Q_2$)

$$I = (Q_1 \cap Q_2) \cap \cdots \cap Q_n = Q_2' \cap Q_3 \cap \cdots \cap Q_n \tag{2}$$

με $\sqrt{Q_2'} = \sqrt{Q_1} \cap \sqrt{Q_2} = P$. Η (2) έχει τώρα $n-1$ όρους. Συνεχίζοντας κατά αυτόν τον τρόπο μπορούμε να αναγάγουμε την (1) σε μια πρωταρχική ανάλυση όπου τα ριζικά $\sqrt{Q_i}$ είναι ανά δύο διάφορα, εξασφαλίζοντας έτσι τη συνθήκη 1) του Ορισμού 11.1.2.

Για τη συνθήκη 2) του ορισμού 11.1.2, παρατηρούμε ότι μπορούμε απλούστατα να παραλείψουμε από την (1) εκείνα τα $Q_j$ για τα οποία ισχύει $I = \bigcap_{i \neq j} Q_i$. Συνεπώς έχουμε το ακόλουθο.

**11.1.4 Πόρισμα** *Κάθε αναλύσιμο ιδεώδες έχει μια τουλάχιστον ελάχιστη πρωταρχική ανάλυση.*

## 11.2 1ο Θεώρημα Μοναδικότητας

Είδαμε στην προηγούμενη παράγραφο τρεις διαφορετικές πρωταρχικές αναλύσεις του ιδεώδους $(x^2, xy) \subseteq k[x, y]$

$$\begin{aligned}(x^2, xy) &= (x) \cap (x, y)^2 \\ &= (x) \cap (x^2, y) \\ &= (x) \cap (x, y)^2 \cap (x^2, y)\end{aligned}$$

από τις οποίες οι πρώτες δύο ήταν ελάχιστες. Παρατηρούμε ότι στις δύο πρώτες ο αριθμός των όρων είναι ο ίδιος και επιπλέον τα αντίστοιχα ριζικά ταυτίζονται: $\sqrt{(x, y)^2} = \sqrt{(x^2, y)} = (x, y)$. Αυτό ακριβώς είναι το περιεχόμενο του επόμενου σημαντικού θεωρήματος.

**11.1.2 1ο Θεώρημα Μοναδικότητας** *Έστω I ένα αναλύσιμο ιδεώδες του R και*

$$I = Q_1 \cap \cdots \cap Q_n, \quad \sqrt{Q_i} = P_i$$

$$I = Q_1' \cap \cdots \cap Q_m', \quad \sqrt{Q_j'} = P_j'$$

*δύο ελάχιστες πρωταρχικές αναλύσεις του I. Τότε*

$$n = m \text{, και } \{P_1, \ldots, P_n\} = \{P_1', \ldots, P_n'\}.$$

Επομένως το πλήθος των όρων σε μια ελάχιστη πρωταρχική ανάλυση όπως και τα ριζικά των πρωταρχικών ιδεωδών δεν εξαρτώνται από τη συγκεκριμένη επιλογή της ελάχιστης πρωταρχικής ανάλυσης.

**11.2.2 Λήμμα** *Έστω Q ένα R – πρωταρχικό ιδεώδες του R και* $a \in R$.
*(i) Αν* $a \in Q$, *τότε* $(Q : a) = R$
*(ii) Αν* $a \notin Q$, *τότε το* $(Q : a)$ *είναι P- πρωταρχικό*
*(iii) Αν* $a \notin P$, *τότε* $(Q : a) = Q$.

**Απόδειξη.** (i) $(Q : a) = \{r \in R \mid ra \in Q\}$, γιατί $a \in Q$.

(ii) Έστω $b \in (Q : a)$. Τότε $ba \in Q$. Αφού $a \notin Q$ και το $Q$ είναι πρωταρχικό έχουμε $b \in \sqrt{Q} = P$. Άρα $Q \subseteq (Q : a) \subseteq P$. Παίρνοντας ριζικά έχουμε

$$P \subseteq \sqrt{(Q:a)} \subseteq \sqrt{P} = P .$$

Άρα $\sqrt{(Q:a)} = P$.

Έστω τώρα $c,d \in R$ με $cd \in (Q:a)$ και $c \notin (Q:a)$. Τότε $c\,d\,a \in Q$ και επειδή το $Q$ είναι πρωταρχικό και $c\,a \notin Q$ έχουμε

$$d \in \sqrt{Q} = P = \sqrt{(Q:a)} .$$

Άρα το $(Q:a)$ είναι πρωταρχικό.

(iii) Αν $b \in (Q:a)$, τότε $ba \in Q$. Αφού $a \neq P = \sqrt{Q}$, έχουμε $b \in Q$.

Άρα

$$(Q:a) \subseteq Q .$$

Η άλλη σχέση υποσυνόλου είναι προφανής. Άρα $(Q:a) = Q$. □

**11.2.3 Θεώρημα** *Έστω $I$ ένα αναλύσιμο ιδεώδες του $R$ και*

$$I = Q_1 \cap \cdots \cap Q_n, \quad \sqrt{Q_i} = P_i$$

*μια ελάχιστη πρωταρχική ανάλυση του $I$. Έστω $P \in \operatorname{Spec} R$. Οι ακόλουθες συνθήκες είναι ισοδύναμες*

*(i)* $P = P_i$ *για κάποιο* $i$

*(ii) υπάρχει* $a \in R$ *με την ιδιότητα* $(I:a)$ *είναι $P$-πρωταρχικό*

*(iii) υπάρχει* $a \in R$ *με την ιδιότητα* $\sqrt{(I:a)} = P$.

**Απόδειξη** (i)$\Rightarrow$(ii) Έστω $P = P_i$ για κάποιο $i$. Επειδή η πρωταρχική ανάλυση $I = Q_1 \cap \cdots \cap Q_n$ είναι ελάχιστη υπάρχει

$$a_i \in \bigcap_{j \neq i} Q_j - Q_i .$$

Σύμφωνα με την Άσκηση 0.6 έχουμε

$$(I:a_i) = (Q_1 \cap \cdots \cap Q_n : a_i) = (Q_i : a_i) \cap \ldots \cap (Q_n : a_i) .$$

Από το Λήμμα 11.2.2 έχουμε

$$(Q_j : a_i) = \begin{cases} R \text{ αν } j \neq i \\ \text{είναι } P_i - \text{πρωταρχικό αν } j = i \end{cases}$$

Τώρα παίρνουμε από τις δύο προηγούμενες σχέσεις ότι $(I : a_i) = (Q_i : a_i)$ που είναι ένα $P = P_i$-πρωταρχικό ιδεώδες.

(ii) $\Rightarrow$ (iii) Άμεσο από τον ορισμό.

(iii) $\Rightarrow$ (i) Έστω $\sqrt{(I : a)} = P$. Όπως και πριν έχουμε

$$(I : a) = (Q_1 : a) \cap \cdots \cap (Q_n : a)$$

οπότε παίρνοντας ριζικά έχουμε (Άσκηση 6.1)

$$P = \sqrt{(Q_1 : a)} \cap \cdots \cap \sqrt{(Q_n : a)}$$

Με τη βοήθεια του Λήμματος 11.2.2 i) η προηγούμενη σχέση γράφεται

$$P = \bigcap_{a \notin Q_i} \sqrt{(Q_1 : a)},$$

οπότε το Λήμμα 11.2.2 ii) δίνει

$$P = \bigcap_{a \notin Q_i} P_i.$$

Τώρα από το Λήμμα 6.1.3 ii) παίρνουμε $P = P_i$ για κάποιο $i$. □

Το προηγούμενο θεώρημα μας πληροφορεί ότι σε κάθε ελάχιστη πρωταρχική ανάλυση του αναλύσιμου ιδεώδους $I$ τα ριζικά των πρωταρχικών όρων είναι τα πρώτα ιδεώδη του $R$ που έχουν τη μορφή $\sqrt{(I : a)}, a \in R$.

**Απόδειξη θεωρήματος 11.2.1** Άμεση από την προηγούμενη παρατήρηση, γιατί τα πρώτα ιδεώδη της μορφής $\sqrt{(I : a)}$ εξαρτώνται μόνο από το $I$ (και όχι από τις ελάχιστες πρωταρχικές αναλύσεις του). □

Το Θεώρημα 11.2.1 μας επιτρέπει να δώσουμε τον εξής ορισμό.

**11.2.4 Ορισμός** *Έστω $I$ ένα αναλύσιμο ιδεώδες του $R$ και*

$$I = Q_1 \cap \cdots \cap Q_n, \quad \sqrt{Q_i} = P_i$$

*μια ελάχιστη πρωταρχική ανάλυση του I. Με* $\operatorname{Ass} I$ *συμβολίζουμε το σύνολο*

$$\operatorname{Ass} I = \{P_1, \ldots, P_n\} \subseteq \operatorname{Spec} R.$$

*Θα λέμε ότι το $P \in \operatorname{Ass} I$ είναι αντίστοιχο πρώτο ιδεώδες του $I$ ή το $P$ αντιστοιχεί στο $I$.*

Σύμφωνα με το $1^{ο}$ Θεώρημα μοναδικότητας το σύνολο $\operatorname{Ass} I$ δεν εξαρτάται από την εκλογή της ελάχιστης πρωταρχικής ανάλυσης του *I*, αλλά μόνο από το *I*.

## 11.3 $2^{ο}$ Θεώρημα Μοναδικότητας

Έστω *I* ένα αναλύσιμο ιδεώδες του *R*. Είδαμε στην προηγούμενη παράγραφο ότι αν

$$I = Q_1 \cap \cdots \cap Q_n, \quad \sqrt{Q_i} = P_i$$

είναι μια ελάχιστη πρωταρχική ανάλυση του *I*, τότε το σύνολο $\{P_1, \ldots, P_n\} = \operatorname{Ass} I$ δεν εξαρτάται από την επιλογή της συγκεκριμένης ελάχιστης ανάλυσης. Εύλογο είναι λοιπόν το ερώτημα αν τα $Q_i$ είναι μοναδικά. Γρήγορα βλέπουμε ότι η απάντηση είναι αρνητική:

$$\begin{aligned}(x^2, xy) &= (x) \cap (x, y)^2 \\ &= (x) \cap (x^2, y)\end{aligned}$$

είναι δύο ελάχιστες πρωταρχικές αναλύσεις του $(x^2, xy)$ στο $k[x, y]$, όπως είδαμε στην §11.1. Όμως δεν είναι τυχαίο που το πρωταρχικό ιδεώδες $(x)$ εμφανίζεται και στις δύο αναλύσεις. Θα δούμε στα επόμενα ότι *κάποια* από τα $Q_i$ είναι μοναδικά ($2^{ο}$ Θεώρημα μοναδικότητας). Για το σκοπό αυτό χρειαζόμαστε την έννοια του ελαχίστου πρώτου ιδεώδους, που διαπραγματευόμαστε αμέσως παρακάτω.

Έστω *I* ένα γνήσιο ιδεώδες του δακτυλίου *R*. Θέτουμε

$$\operatorname{Var}(I) = \{P \in \operatorname{Spec} R \mid P \supseteq I\}$$

**11.3.1 Πρόταση** *Το σύνολο* $\operatorname{Var}(I)$, *όπου I είναι γνήσιο ιδεώδες του R, περιέχει ένα τουλάχιστον ελάχιστο στοιχείο*.

**Απόδειξη** Θα χρησιμοποιήσουμε το λήμμα του Zorn (Λήμμα 3.5.1). Αρχικά παρατηρούμε ότι $\operatorname{Var}(I) \neq \varnothing$ λόγω του Πορίσματος 3.5.3. Ορίζουμε στο σύνολο $\operatorname{Var}(I)$ τη μερική διάταξη

$$P_1 \leq P_2 \Leftrightarrow P_1 \supseteq P_2$$

(μεγαλύτερα στοιχεία είναι υποσύνολα). Έστω ολικά διατεταγμένο $\Omega \subseteq \operatorname{Var}(I)$ με $\Omega \neq \varnothing$. Θέτουμε

$$Q = \bigcap_{P \in \Omega} P .$$

Τότε $Q \neq R$ αφού $P \neq R (P \in \Omega \neq \varnothing)$. Θα δείξουμε ότι $Q \in \operatorname{Spec} R$. Έστω $a, b \in R$ με $ab \in Q$ και $a \neq Q$. Τότε υπάρχει $P_1 \in \Omega$ με $a \neq P_1$. Το $\Omega$ είναι ολικά διατεταγμένο. Άρα για $P \in \Omega$ ισχύει $P_1 \subseteq P$ ή $P \subseteq P_1$. Στην πρώτη περίπτωση έχουμε $ab \in Q \Rightarrow ab \in P_1 \Rightarrow b \in P_1$ γιατί του $P_1$ είναι πρώτο και $a \neq P_1$. Άρα $b \in P$. Επίσης και στη δεύτερη περίπτωση ισχύει $b \in P$. Συνεπώς $b \in Q$. Αποδείξαμε ότι $Q \in \operatorname{Spec} R$ και κατά συνέπεια $Q \in \operatorname{Var}(I)$. Το $Q$ είναι έτσι ένα άνω φράγμα του $\Omega$ στο $\operatorname{Var}(I)$. Από το λήμμα του Zorn προκύπτει τώρα η ύπαρξη ενός μέγιστου στοιχείου του $\operatorname{Var}(I)$ ως προς τη μερική διάταξη $\leq$. □

**11.3.2 Ορισμός** *Έστω $I$ ένα γνήσιο ιδεώδες του δακτυλίου $R$. Κάθε ελάχιστο στοιχείο του $\operatorname{Var}(I)$ ονομάζεται ελάχιστο πρώτο ιδεώδες του $I$. Το σύνολο των ελάχιστων πρώτων ιδεωδών του $I$ συμβολίζεται με $\min(I)$.*

Μια γενίκευση της Πρότασης 11.3.1 θα μας είναι ιδιαίτερα χρήσιμη.

**11.3.3 Πρόταση** *Έστω $P$ ένα πρώτο ιδεώδες του $P$ και $I$ ιδεώδες $P \subseteq I$. Τότε το σύνολο*

$$\{P' \in \operatorname{Spec} R \mid P \supseteq P' \supseteq I\}$$

*περιέχει ένα τουλάχιστον ελάχιστο στοιχείο.*

**Απόδειξη** Η απόδειξη είναι παρόμοια με εκείνη της Πρόταση 11.3.1: στο σύνολο $\{P' \in \operatorname{Spec} R \mid P \supseteq P' \supseteq I\}$ ορίζουμε τη μερική διάταξη

$$P_1 \leq P_2 \Leftrightarrow P_1 \supseteq P_2$$

και εφαρμόζουμε το λήμμα του Zorn. Αφήνουμε τις λεπτομέρειες ως άσκηση. □

Επιστρέφουμε τώρα στις πρωταρχικές αναλύσεις ιδεωδών.

**11.3.4 Πρόταση** *Έστω $I$ ένα αναλύσιμο ιδεώδες του $R$ και $P \in Spec R$. Τότε*

$$P \in \min(I) \Leftrightarrow P \text{ είναι ελάχιστο στοιχείο του } \operatorname{Ass} I .$$

*Κατά συνέπεια το σύνολο* $\min(I)$ *είναι πεπερασμένο*

**Απόδειξη** Ισχυρισμός: Ισχύει $P \supseteq I \Leftrightarrow P \supseteq P'$ για κάποιο $P' \in \operatorname{Ass} I$. Πράγματι, έστω $I = Q_1 \cap \cdots \cap Q_n$, $\sqrt{Q_i} = P_i$ μια ελάχιστη πρωταρχική ανάλυση του *I*. Έχουμε τότε

$$\sqrt{I} = \sqrt{Q_1} \cap \ldots \cap \sqrt{Q_n} = P_1 \cap \ldots \cap P_n$$

(Άσκηση 6.1), οπότε από το Λήμμα 6.1.3 ii) συμπεραίνουμε ότι $P \supseteq I \Leftrightarrow P \supseteq \sqrt{P} \supseteq \sqrt{I} \Leftrightarrow P \supseteq P_i$ για κάποιο $i \Leftrightarrow P \supseteq P'$ για κάποιο $P' \in \operatorname{Ass} I$, που είναι το ζητούμενο.

"$\Rightarrow$" Έστω $P \in \min(I)$. Τότε από τον ισχυρισμό έχουμε $P \supseteq P'$ για κάποιο $P' \in \operatorname{Ass}(I)$. Αφού $P \in \min(I)$ έχουμε $P = P'$. Άρα το *P* είναι ελάχιστο στοιχείο του $\operatorname{Ass}(I)$.

"$\Leftarrow$" Έστω *P* ελάχιστο στοιχείο του $\operatorname{Ass}(I)$. Τότε $P \supseteq I$. Από την Πρόταση 11.3.3 υπάρχει $P' \in \min(I)$ με την ιδιότητα $P \supseteq P' \supseteq I$. Εφαρμόζουμε τον ισχυρισμό στο $P' \supseteq I$ και συμπεραίνουμε ότι υπάρχει $P'' \in \operatorname{Ass}(I)$ με την ιδιότητα $P' \supseteq P''$. Από τις σχέσεις $P \supseteq P' \supseteq P''$ και την υπόθεση στο *P* έπεται ότι $P' = P''$. Άρα $P = P' \in \min(I)$. □

**11.3.5 Θεώρημα (2ο Θεώρημα Μοναδικότητας)** *Έστω I ένα αναλύσιμο ιδεώδες του δακτυλίου R και* $\operatorname{Ass}(I) = \{P_1, \ldots, P_n\}$. *Έστω*

$$I = Q_1 \cap \cdots \cap Q_n, \quad \sqrt{Q_i} = P_i$$
$$I = Q_1' \cap \cdots \cap Q_n', \quad \sqrt{Q_j'} = P_i'$$

δύο ελάχιστες πρωταρχικές αναλύσεις του *I*. Τότε για κάθε $P_i \in \min(I)$ ισχύει $Q_i = Q_i'$.

**Απόδειξη** Έστω $n > 1$ και (χωρίς βλάβη της γενικότητας) $P_1 \in \min(I)$. Λόγω του Λήμματος 6.1.3 και της υπόθεσης στο $P_i$, υπάρχει

$$a \in P_2 \cap \ldots \cap P_n - P_1.$$

Για κάθε $j = 2,3,\ldots,n$ υπάρχει $m_j \in \mathbb{N}$ με την ιδιότητα $a^{m_j} \in Q_j$. Έστω $t = \max\{m_2,\ldots,m_n\}$. Τότε $a^t \notin P_1$ και το Λήμμα 11.2.2 (i), (iii) δίνει

$$(I : a^t) = (Q_1 \cap \cdots \cap Q_n : a^t) = (Q_i : a^t) \cap \ldots \cap (Q_n : a^t) = Q_1.$$

Συνεπώς $Q_1 = (I : a^t)$ για αρκετά μεγάλο *t*. Με παρόμοιο τρόπο, $Q_1' = (I : a^t)$ για αρκετά μεγάλο *t*. Έτσι λοιπόν $Q_1 = Q_1'$. □

**Σημείωση** Στη διατύπωση του 2ου θεωρήματος μοναδικότητας, θα μπορούσαμε να αντικαταστήσουμε τη συνθήκη "$P_i \in \mathrm{Min}(I)$" με "$P_i$ είναι ελάχιστο στοιχείο του συνόλου $\{P_1,\ldots,P_n\}$", οπότε η ίδια απόδειξη (με την προφανή αντικατάσταση της συνθήκης στην πρώτη γραμμή) εξακολουθεί να ισχύει. Όμως η πρώτη συνθήκη είναι σαφώς προτιμότερη γιατί δεν αναφέρεται σε πρωταρχικές αναλύσεις.

Στην Πρόταση 6.3.3 είδαμε ότι κάθε ανάγωγο ιδεώδες δακτυλίου του Noether είναι πρωταρχικό. Στην Άσκηση 4.3 είδαμε ότι κάθε γνήσιο ιδεώδες δακτυλίου της Noether είναι τομή πεπερασμένου πλήθους ανάγωγων ιδεωδών. Συνεπώς έχουμε το εξής θεώρημα.

**11.3.6 Θεώρημα (Lasker-Noether)** *Έστω R δακτύλιος της Noether. Τότε κάθε γνήσιο ιδεώδες του R είναι αναλύσιμο.* □

## 11.4 Εφαρμογή: Θεώρημα τομής του Krull

Χρησιμοποιώντας πρωταρχική ανάλυση ιδεωδών ο Krull (1938) απέδειξε το εξής θεώρημα.

**11.4.1 Θεώρημα τομής του Krull** *Έστω R ένας τοπικός δακτύλιος της Noether με μέγιστο ιδεώδες το* $\underline{m}$. *Τότε*

$$\bigcap_{n\geq 1} \underline{m}^n = 0.$$

Για την απόδειξη χρειαζόμαστε την επόμενη πρόταση.

**11.4.2 Πρόταση** *Έστω I ένα ιδεώδες του δακτυλίου της Noether R. Τότε*

$$\left(\bigcap_{n\geq 1} I^n\right) I = \bigcap_{n\geq 1} I^n$$

**Απόδειξη** Μπορούμε να υποθέσουμε ότι το $I$ είναι γνήσιο, οπότε θέτοντας

$$J = \bigcap_{n\geq 1} I^n$$

βλέπουμε ότι και $JI$ είναι γνήσιο αφού $JI \subseteq I$. Από το θεώρημα 11.3.6, το $JI$ έχει μια πρωταρχική ανάλυση. Έστω λοιπόν

$$JI = Q_1 \cap \cdots \cap Q_n, \quad \sqrt{Q_i} = P_i$$

μια ελάχιστη πρωταρχική ανάλυση. Επειδή $JI \subseteq J$ αρκεί να δείξουμε ότι $J \subseteq JI$ και αυτό θα πραγματοποιηθεί δείχνοντας ότι $J \subseteq Q_i$ για κάθε $i$.

Για άτοπο, έστω $J \not\subset Q_i$ για κάποιο $i$. Έστω $a \in J - Q_i$. Ισχύει

$$aI \subseteq Q_i .$$

Επειδή το $Q_i$ είναι πρωταρχικό, παίρνουμε $I \subseteq \sqrt{Q_i} = P_i$. Όμως από το λήμμα 6.1.4 έχουμε $P_i^t \subseteq Q_i$ για κάποιο $t$. Συνεπώς

$$\bigcap_{n\geq 1} I^n \subseteq I^t \subseteq P_i^t \subseteq Q_i ,$$

που είναι βέβαια άτοπο. □

**Απόδειξη του θεωρήματος 11.4.1** Έστω $J = \bigcap_{n\geq 1} \underline{m}^n$. Από την προηγούμενη πρόταση παίρνουμε

$$J\underline{m} = J .$$

Ως $R$-πρότυπο, το $J$ είναι πεπερασμένα παραγόμενο αφού ο $R$ είναι της Noether. Επομένως ισχύει το λήμμα του Nakayama (Πόρισμα 7.1.4) απ' όπου συμπεραίνουμε ότι $J = 0$. □

## Ασκήσεις

**1.** Το γνήσιο ιδεώδες $I$ του $R$ είναι πρωταρχικό αν και μόνο αν κάθε μηδενοδιαιρέτης του $R/I$ είναι μηδενοδύναμος ($ab = 0$ στο $R/I$ με $a \neq 0 \Rightarrow a^m = 0$ για κάποιο $m > 0$).

**2.** Έστω $f : R \to S$ ομομορφισμοί δακτυλίων και $Q$ ένα $P$-πρωταρχικό ιδεώδες του $S$. Τότε το $f^{-1}(Q)$ είναι $f^{-1}(P)$ -πρωταρχικό ιδεώδες του $R$.

**3.** Έστω $f : R \to R[x]$ ο φυσικός μονομορφισμός. Έστω $Q$ και $I$ ιδεώδη του $R$. Με $Q^e$ συμβολίζουμε την επέκταση του $Q$ στο $R[x]$ (Κεφάλαιο 10).

(i) $Q$ πρωταρχικό $\Leftrightarrow Q^e$ πρωταρχικό ιδεώδες του $R[x]$

(ii) Αν το $I$ είναι αναλύσιμο και

$$I = Q_1 \cap \cdots \cap Q_n, \quad \sqrt{Q_i} = P_i$$

είναι μια πρωταρχική ανάλυση του $I$, τότε

$$I^e = Q_1^e \cap \cdots \cap Q_n^e, \quad \sqrt{Q_1^e} = P_i^e$$

είναι μια πρωταρχική ανάλυση του $I^e$.

(iii) Αν το $I$ είναι αναλύσιμο τότε

$$\mathrm{Ass}_{R[x]} I^e = \{P^e : P \in \mathrm{Ass}\, I\}.$$

**4.** Έστω $k$ σώμα και $a_1, \ldots, a_n \in k$. Το ιδεώδες

$$((x_1 - a_1)^{t_1}, \ldots, (x_n - a_n)^{t_n})$$

είναι πρωταρχικό για κάθε $t_i \in \mathbb{N}$.

**5.** Έστω $Q$ ένα $P$ – πρωταρχικό ιδεώδες του $R$ και $S \subseteq R$ ένα πολλαπλασιαστικό υποσύνολο.

(i) $Q \cap S = \varnothing \Leftrightarrow P \cap S = \varnothing$

(ii) Έστω $Q \cap S = \varnothing$. Έστω $\lambda \in Q^e$ (συμβολισμός κεφαλαίου 10) με $\lambda = r/s (r \in R, s \in S)$. Τότε $r \in Q$. Επιπλέον $Q^{ec} = Q$.

(iii) Αν $Q \cap S = \varnothing$, τότε το $Q^e$ είναι $P^e$ - πρωταρχικό ιδεώδες του $S^{-1}R$

(v) Αν $Q'$ είναι $P'$ - πρωταρχικό ιδεώδες του $S^{-1}R$, τότε το $(Q')^c$ είναι $(P')^c$ - πρωταρχικό ιδεώδες του $R$ και $(Q')^c \cap S = \varnothing$. Επιπλέον $(Q')^{ce} = Q'$.

(vi) Συμπέρασμα: κάθε πρωταρχικό ιδεώδες του $S^{-1}R$ είναι της μορφής $Q^e$ για μοναδικό πρωταρχικό ιδεώδες $Q$ του $R$ με την ιδιότητα $Q \cap S = \varnothing$.

**6.** Έστω $R$ ένας δακτύλιος της Noether και $I$ ένα ιδεώδες του $R$. Τότε το σύνολο των μηδενοδιαιρέτων του $R/I$ είναι

$$\bigcup_{P\in \mathrm{Ass}\, I} P .$$

Υπόδειξη: για τη σχέση $\subseteq$ θεωρήσετε μια ελάχιστη πρωταρχική ανάλυση του $I$. Για τη σχέση "$\supseteq$" έστω $P \in \mathrm{Ass}\, I$. Τότε το $(I : a)$ είναι $P$-πρωταρχικό για κάποιο $a$ (Θεώρημα 11.2.3). Για κάποιο $t$ έχουμε $r^t a \in I$.

**7.** (Θεώρημα τομής του Krull). Έστω $R$ δακτύλιος της Noether και $Jac(R)$ η τομή των μέγιστων ιδεωδών του $R$. Έστω $I \subseteq \mathrm{Jac}(R)$. Τότε

$$\bigcap_{n=1}^{\infty} I^n = 0$$

Υπόδειξη: Αποδείξετε την ακόλουθη γενίκευση του λήμματος του Nakayama: αν $M$ είναι πεπερασμένα παραγόμενο $R$-πρότυπο και $M = IM$, όπου $I \subseteq \mathrm{Jac}(R)$, τότε $M = 0$. Τώρα συνεχίσετε όπως στο θεώρημα 11.4.1.

**8.** Έστω $R$ τοπικός δακτύλιος της Noether με μέγιστο ιδεώδες $m$.

(i) Αν $\mathrm{Spec}\, R \neq \{m\}$ τότε $m^{n+1} \underset{\neq}{\subset} m^n$ για κάθε $n$.

(ii) Αν $I$ είναι ιδεώδες με $\sqrt{I} \neq m$, τότε $I + m^{n+1} \underset{\neq}{\subset} m^n$ για κάθε $n$.

**9.** Στο $\mathbb{Z}[x]$ αποδείξετε ότι οι παρακάτω είναι πρωταρχικές αναλύσεις. Ποιες είναι οι ελάχιστες;

$$\begin{aligned} (4, 2x, x^2) &= (4, x) \cap (2, x^2) \\ (9, 3x+3) &= (3) \cap (9, x+1) \end{aligned}$$

**10.** Προσδιορίστε μια πρωταρχική ανάλυση του $I = (xy, x - yz) \subseteq k[x, y, z]$.

Υπόδειξη: ποια είναι η ομοπαραλληλική πολλαπλότητα $V(I)$;

**11.** Έστω $R$ περιοχή της Noether. Αποδείξετε ότι είναι περιοχή μοναδικής παραγοντοποίησης αν και μόνο αν κάθε ελάχιστο πρώτο ιδεώδες κάθε κυρίου ιδεώδους είναι κύριο.

Υπόδειξη: Άσκηση 1.8.

**12.** Έστω $R$ περιοχή της Noether όπου κάθε μέγιστο ιδεώδες είναι πρώτο. Τότε κάθε μη μηδενικό ιδεώδες του $R$ γράφεται ως γινόμενο πρωταρχικών ιδεωδών των οποίων τα ριζικά είναι ανά δύο διάφορα. Η παράσταση είναι μοναδική.

**13.** Έστω $I$ γνήσιο ριζικό ιδεώδες ενός δακτυλίου της Noether. Αποδείξετε ότι το $I$ γράφεται μοναδικά ως τομή πεπερασμένου πλήθους πρώτων ιδεωδών. Ποια είναι η γεωμετρική ερμηνεία όταν $R = k[x_1, \ldots, x_n]$; (Δες την Πρόταση 8.1.5 (ii) και Άσκηση 8.20).

**14.** Έστω $R = k[x, y]/(x^2, xy)$ και $a, b \in R$ οι εικόνες των $x, y$. Τότε το $(b^n)$ είναι $(a,b)$-πρωταρχικό ιδεώδες του $R$ και $0 = (a) \cap (b^n)$ είναι ελάχιστη πρωταρχική ανάλυση του 0 για κάθε $n \geq 1$.

# Κεφάλαιο 12

# Δακτύλιοι Διακριτής Εκτίμησης

Οι δακτύλιοι διακριτής εκτίμησης εμφανίζονται συχνά στην Αλγεβρική Θεωρία Αριθμών (τοπικοποιήσεις του $\mathcal{O}_k$ σε πρώτο ιδεώδες, όπου $k$ είναι αριθμητικό σώμα, Ασκήσεις 6, 7) και στην Αλγεβρική Γεωμετρία (τοπικός δακτύλιος μη ιδιάζουσας επίπεδης καμπύλης, Άσκηση 8). Στο κεφάλαιο αυτό θα δώσουμε ένα χαρακτηρισμό τους.

## 12.1 Διακριτές εκτιμήσεις

Έστω $k$ σώμα. Μια *διακριτή εκτίμηση* του $k$ είναι μια επί συνάρτηση

$$v : k - \{0\} \to \mathbb{Z}$$

που ικανοποιεί τις συνθήκες

(i) $v(xy) = v(x) + v(y)\ \forall x, y \in k - \{0\}$.

(ii) $v(x \pm y) \geq \min\{v(x), v(y)\}\ \forall x, y \in k - \{0\}$.

Φυσικά ισχύει $v(x^{-1}) = -v(x)$ και $v(1) = 0$.

Για παράδειγμα, έστω $p \in \mathbb{Z}$ πρώτος αριθμός. Αν $\frac{a}{b} \in \mathbb{Q} - \{0\}$ με $a, b \in \mathbb{Z}$ θέτουμε $v_p\left(\frac{a}{b}\right) = a_p - b_p$ όπου $a_p$ και $b_p$ είναι οι δυνάμεις του $p$ εμφανίζονται στις παραγοντοποιήσεις των $a$ και $b$ αντίστοιχα. Η συνάρτηση $v_p$ είναι μια διακριτή εκτίμηση του $\mathbb{Q}$ (Άσκηση 1) και ονομάζεται $p$-αδική εκτίμηση.

Έστω $v : k - \{0\} \to \mathbb{Z}$ μια διακριτή εκτίμηση. Το σύνολο

$$R = \{a \in k \mid v(a) \geq 0\}$$

είναι υποδακτύλιος του *k*. Κάθε τέτοιος δακτύλιος καλείται *δακτύλιος διακριτής εκτίμησης*. Το σύνολο

$$\underline{m} = \{a \in k \mid v(a) > 0\}$$

είναι ιδεώδες του *R*, όπως φαίνεται αμέσως από τις συνθήκες i) και ii).

**12.1.1 Πρόταση** *Έστω k σώμα και v διακριτή εκτίμηση του k. Τότε*

*(i) Ο δακτύλιος* $R = \{a \in k \mid v(a) \geq 0\}$ *είναι τοπικός δακτύλιος με μέγιστο ιδεώδες το* $\underline{m} = \{a \in k \mid v(a) > 0\}$.

*(ii) Ο R είναι της Noether.*

*(iii)Αν υπάρχει* $t \in R$ *με* $v(t) = 1$ *τέτοιο ώστε:* $\underline{m} = (t)$, *κάθε* $a \in R$ *γράφεται* $a = t^n u$ *με* $n \in \mathbb{N}$ *και u αντιστρέψιμο στοιχείο του R, και κάθε ιδεώδες του R είναι της μορφής* $I = (t^m)$ *για κάποιο* $m \in \mathbb{N}$.

**Απόδειξη** (i) Επειδή το $\underline{m}$ είναι ιδεώδες, για να δείξουμε το (i) αρκεί να δείξουμε ότι κάθε $a \in R - \underline{m}$ είναι αντιστρέψιμο στο *R*. Έστω $a \in R - \underline{m}$. Τότε $v(a) = 0$. Έχουμε $a^{-1} \in k$ και $v(aa^{-1}) = v(1) = 0 \Rightarrow v(a^{-1}) = -v(a)$. Άρα $v(a^{-1}) = 0$, δηλαδή $a^{-1} \in R$.

(ii) Έπεται προφανώς από το iii) (κάθε ιδεώδες είναι πεπερασμένα παραγόμενο).

(iii) Έστω $t \in R$ *με* $v(t) = 1$ (η *v* είναι επί συνάρτηση). Αν $a \in \underline{m}$ τότε $v(a) > 0 \Rightarrow v(a) \geq 1 \Rightarrow v(a) - v(t) \geq 0 \Rightarrow v(a) - v(t) \geq 0 \Rightarrow v(at^{-1}) \geq 0 \Rightarrow at^{-1} \in R \Rightarrow a \in (t)$. Άρα $\underline{m} \subseteq (t)$. Επειδή το *m* είναι μέγιστο και $(t) \neq R$ (αφού το *t* δεν είναι αντιστρέψιμο του *R* έχουμε $\underline{m} = (t)$. Ισχύει $a = t^{v(a)}u$ για κάποιο αντιστρέψιμο $u \in R$. Πράγματι, αυτό είναι προφανές για *a* αντιστρέψιμο στο *R*, αφού τότε $v(a) = 0$. Υποθέτουμε λοιπόν ότι $a \in \underline{m}$. Για το στοιχείο $u = at^{-v(a)} \in k$ έχουμε $v(u) = v(a) - v(a) = 0$. Άρα το *u* είναι αντιστρέψιμο στο *R*. Έτσι $a = t^{v(a)}u$. Για τον τελευταίο ισχυρισμό του (iii), έστω *I* ιδεώδες του *R*. Θέτουμε

$$m = \min\{v(a) \mid a \in I\}.$$

Ισχύει $I = (t^m)$. Πράγματι, η σχέση $(t^m) \subseteq I$ είναι προφανής. Έστω $a \in I$. Τότε σύμφωνα μ' αυτό που αποδείξαμε πριν έχουμε $a = t^{v(a)}u$ για κάποιο αντιστρέψιμο $u \in R$. Ισχύει $v(a) \geq m$ και άρα $a \in (t^m)$. □

Ένα στοιχείου $t$ όπως στην προηγούμενη πρόταση, ονομάζεται *τοπική παράμετρος* της εκτίμησης $v$. Για παράδειγμα, μια τοπική παράμετρο της $p$-αδικής εκτίμησης $v_p$ του $\mathbb{Q}$ είναι το στοιχείο $t = p$.

**12.1.2 Παρατήρηση** Από την προηγούμενη πρόταση βλέπουμε ότι κάθε δακτύλιος διακριτής εκτίμησης είναι περιοχή κυρίων ιδεωδών και άρα περιοχή μοναδικής παραγοντοποίησης (Θεώρημα 1.2.1). Το στοιχείο $t$ είναι ανάγωγο. Άρα το πρόβλημα της εύρεσης της ανάγωγης παραγοντοποίησης του $a \in R - \underline{m}$ ανάγεται στον προσδιορισμό του $v(a)$ γιατί $a = t^{v(a)}u$.

## 12.2 Χαρακτηρισμός δακτυλίων διακριτής εκτίμησης

Θα δώσουμε έναν χαρακτηρισμό των δακτυλίων διακριτής εκτίμησης που αποτελεί το κύριο αποτέλεσμα αυτού του κεφαλαίου. Χρειαζόμαστε την έννοια της κανονικής περιοχής: μια περιοχή $R$ ονομάζεται *κανονική* αν $R = \overline{R}$, όπου $\overline{R}$ είναι η ακέραιη θήκη του $R$ στο σώμα πηλίκων του (Ορισμός 7.2.4). Δηλαδή η $R$ είναι κανονική αν περιέχει κάθε στοιχείο του σώματος των πηλίκων του που είναι ακέραιο πάνω από το $R$. Από την Παρατήρηση 12.1.2 και την Άσκηση 7.7 γνωρίζουμε ότι κάθε δακτύλιος διακριτής εκτίμησης είναι κανονικός.

**12.2.1 Θεώρημα** *Έστω $R$ ένας δακτύλιος. Τότε ο $R$ είναι δακτύλιος διακριτής εκτίμησης αν και μόνο αν ισχύουν οι συνθήκες*

*(i)* *$R$ είναι της Noether.*

*(ii)* *$R$ είναι κανονικός.*

*(iii)* $\operatorname{Spec} R = \{0, \underline{m}\}$.

Για την απόδειξη χρειαζόμαστε δύο λήμματα.

**12.2.2 Λήμμα** *Έστω R περιοχή της Noether και* $t = R$. *Αν το t δεν είναι αντιστρέψιμο ισχύει*

$$\bigcap_{n\geq 1}(t^n) = 0$$

**Απόδειξη** Έστω $\bigcap_{n\geq 1}(t^n) = 0$, $x \neq 0$. Τότε

$$x = tx_1 = t^2 x_2 = \ldots$$

για κάποια $x \in R$. Παρατηρούμε ότι

$$(x) \subseteq (x_1) \subseteq (x_2) \subseteq \ldots \qquad (1)$$

και επιπλέον $(x_i) \underset{\neq}{\subset} (x_{i+1})$ για κάθε *i*, γιατί διαφορετικά θα είχαμε $x_{i+1} = ax_i$, όπου $a \in R$, οπότε $x = t^i x_i = t^{i+1} x_{i+1} \Rightarrow t^i x_i = t^{i+1} a x_i \Rightarrow 1 = ta$, που είναι βέβαια άτοπο. Άρα η (1) είναι γνήσια αύξουσα ακολουθία ιδεωδών του *R*, άτοπο. □

**12.2.3 Λήμμα** *Έστω R τοπική περιοχή της Noether, με μέγιστο ιδεώδες το* $\underline{m}$. *Έστω ότι το* $\underline{m}$ *είναι κύριο,* $\underline{m} = (t), t \neq 0$. *Τότε ο R είναι δακτύλιος διακριτής εκτίμησης.*

**Απόδειξη** Έστω $a \in R - \{0\}$ με *a* όχι αντιστρέψιμο. Τότε $a \in \underline{m} = (t)$. Θεωρούμε την ακολουθία ιδεωδών $(t) \supseteq (t^2) \supseteq (t^3) \supseteq \ldots$. Λόγω του Λήμματος 12.2.1 υπάρχει $n \in \mathbb{N}$ με $a \in (t^n), a \notin (t^{n+1})$. Τότε $a = t^n u$ με $u \notin (t)$, οπότε το *u* είναι αντιστρέψιμο. Θα ορίσουμε τώρα μια διακριτή εκτίμηση

$$v : k - \{0\} \to \mathbb{Z},$$

όπου *k* είναι το σώμα πηλίκων του *R*. Αν $a, b \in R - \{0\}$ με $a \in t^m u$, $b = t^n v$ ($u, v$ αντιστρέψιμα στο *R*) θέτουμε

$$v\left(\frac{a}{b}\right) = m - n.$$

Εύκολο επαληθεύεται ότι η *v* είναι καλά οριζόμενη και επί. Επιπλέον ισχύει $v(xy) = v(x) + v(y)$ για κάθε $x, y \in k - \{0\}$. Για την άλλη συνθήκη του ορισμού, έστω ότι ισχύει $v(x) \geq v(y)$. Αν $y = 0$, προφανώς $v(x \pm y) = v(x) \geq v(y)$. Έστω

$y \neq 0$. Τότε $x/y \in R$, αφού $v(x/y) = v(x) - v(y) \geq 0$. Άρα $x/y = t^k u$, $u$ αντιστρέψιμο στο $R$. Τότε

$$\frac{x \pm y}{y} = t^k u \pm 1 \in R$$

Άρα $v\left(\frac{x \pm y}{y}\right) \geq 0$, δηλαδή $v\left(\frac{x}{y}\right) \geq v(y)$. Αποδείξαμε ότι η συνάρτηση $v$ είναι διακριτή εκτίμηση του $k$. Τέλος παρατηρούμε ότι

$$R = \{x \in k \mid v(x) \geq 0\}. \qquad \square$$

**Απόδειξη του θεωρήματος 12.2.1** "$\Rightarrow$" Έστω ότι ο $R$ είναι δακτύλιος διακριτής εκτίμησης. Από την Πρόταση 12.1.1 (ii), ο $R$ είναι της Noether. Είναι επίσης κανονικός όπως είδαμε στην αρχή της § 12.2. Τέλος από την Πρόταση 12.1.1 (iii) έπεται ότι $\operatorname{Spec} R = \{0, (t)\}$.

"$\Rightarrow$" Έστω ότι ισχύουν οι συνθήκες i), ii), iii) του θεωρήματος. Πρώτα παρατηρούμε ότι ο $R$ είναι περιοχή αφού $0 \in \operatorname{Spec} R$. Σύμφωνα με το Λήμμα 12.2.3, αρκεί να δείξουμε ότι το μέγιστο ιδεώδες $\underline{m}$ είναι κύριο.

Έστω $k$ το σώμα πηλίκων του $R$.

*Ισχυρισμός 1* $\underline{m} \neq \underline{m}^2$.

Αυτό έπεται αμέσως από το λήμμα του Nakayama (Πόρισμα 7.1.4), γιατί το $\underline{m}$ είναι πεπερασμένα παραγόμενο (ο $R$ είναι της Noether) και $\underline{m} \neq 0$.

*Ισχυρισμός 2* Έστω $x \in \underline{m} - \underline{m}^2$. Αν $(x) \neq \underline{m}$, τότε υπάρχει $0 \neq y \in \underline{m}$ με την ιδιότητα $y\underline{m} \subseteq (x)$.

Από την Πρόταση 6.1.2 έχουμε $\sqrt{(x)} = \underline{m}$. Από το Λήμμα 6.1.4 παίρνουμε

$$\underline{m}^n \subseteq (x) \subseteq \underline{m}$$

για κάποιο $n \geq 1$. Έστω $n$ ελάχιστος τέτοιος αριθμός, οπότε $\underline{m}^{n-1} \not\subseteq (x)$. Από την υπόθεση έχουμε $n > 1$. Έστω $y \in \underline{m}^{n-1} - (x)$. Τότε βέβαια $y\underline{m} \subseteq m^n \subseteq (x)$.

Θεωρούμε τώρα το στοιχείο $y/x \in k$ (με τις υποθέσεις του Ισχυρισμού 2). Τότε το σύνολο $(y/x)\underline{m}$ είναι ιδεώδες του $R$.

*Περίπτωση α* Έστω $(y/x)\underline{m} = R$. Τότε $yy'/x = 1$ για κάποιο $y' \in \underline{m}$. Άρα $x = yy' \in \underline{m}^2$, άτοπο.

*Περίπτωση β* Έστω $(y/x)\underline{m} \neq R$. Τότε $(y/x)\underline{m} \subseteq \underline{m}$ (Πόρισμα 3.5.3). Από την Πρόταση 7.1.1 συμπεραίνουμε ότι υπάρχει $z \in \underline{m}, z \neq 0$ τέτοιο ώστε

$$[(y/x)^m + a_1(y/x)^{m-1} + \cdots + a_{m-1}(y/x) + a_m]z = 0.$$

Άρα $x/y$ είναι ακέραιο επί του *R*. Από την υπόθεση, ο *R* είναι κανονικός. Άρα $y/x \in R$. Συνεπώς $y \in (x)$, που είναι άτοπο. Και στις δύο περιπτώσεις καταλήξαμε σε άτοπο γιατί υποθέσαμε (δες τον Ισχυρισμό 2) ότι $(x) \neq \underline{m}$. Άρα $\underline{m} = (x)$. □

## Ασκήσεις

**1.** Έστω $p \in \mathbb{Z}$ ένας πρώτος αριθμός. Αποδείξετε ότι η συνάρτηση $v_p$ που ορίστηκε στην αρχής της §12.1 είναι διακριτή εκτίμηση. Αποδείξετε ότι ο δακτύλιος της $v_p$ είναι η τοπικοποίηση του $\mathbb{Z}$ στο $(p)$. Ποιο είναι το μέγιστο ιδεώδες;

**2.** Έστω *R* τοπικός δακτύλιος της Noether του οποίου το μέγιστο ιδεώδες είναι κύριο $\underline{m} = (t)$. Αποδείξετε ότι είτε ο *R* είναι δακτύλιος διακριτής εκτίμησης είτε $t^n = 0$ για κάποιο *n*.

**3.** Μια περιοχή *R* με σώμα πηλίκων *k* ονομάζεται δακτύλιος εκτίμησης αν: $x \in k - \{0\} \Rightarrow x \in R$ ή $x^{-1} \in R$.

(i) Αποδείξετε ότι κάθε δακτύλιος εκτίμησης είναι τοπικός.

(ii) Έστω *R* ένας δακτύλιος εκτίμησης. Τότε ο *R* είναι δακτύλιος διακριτής εκτίμησης αν και μόνο αν ο *R* είναι της Noether.

**4.** Ο δακτύλιος *R* είναι δακτύλιος διακριτής εκτίμησης αν και μόνο αν ισχύουν οι συνθήκες

(i) *R* είναι τοπικός της Noether (με μέγιστο ιδεώδες το $\underline{m}$).

(ii) $\operatorname{Spec} R = \{0, \underline{m}\}$.

(iii) Η διάσταση του $\underline{m}/\underline{m}^2$ ως $R/\underline{m}$ - διανυσματικός χώρος είναι 1.

**5.** Έστω $k$ ένα σώμα. Τότε η τοπικοποίηση του $k[x]$ στο $(x)$ είναι δακτύλιος διακριτής εκτίμησης. Ποια είναι η διακριτή εκτίμηση;

**6.** Έστω $R$ περιοχή της Noether με την ιδιότητα κάθε μη μηδενικό πρώτο ιδεώδες είναι μέγιστο. Τότε $R$ είναι κανονική $\Leftrightarrow R_p =$ δακτύλιος διακριτής εκτίμησης για κάθε πρώτο ιδεώδες $P$ του $R$. (Ο $R$ με τις προηγούμενες ιδιότητες ονομάζεται *περιοχή του Dedekind*).
Υπόδειξη: Άσκηση 10.10

**7.** Έστω $k$ αριθμητικό σώμα. Τότε ο δακτύλιος $\mathcal{O}_k$ των ακέραιων του $k$ είναι περιοχή του Dedekind.
Υπόδειξη: Έστω $P \neq 0$ πρώτο ιδεώδες του $\mathcal{O}_k$ και $a \in P,\ a \neq 0$. Έστω $N(a)$ ο σταθερός όρος του $Irr(a,\mathbb{Q})$. Ο δακτύλιος $\mathcal{O}_k / N(a)$ είναι πεπερασμένος. Άρα η ακεραία περιοχή $\mathcal{O}_k / P$ είναι πεπερασμένη.
Σε περιοχές του Dedekind αποδεικνύεται ότι κάθε ιδεώδες γράφεται ως γινόμενο πεπερασμένου πλήθους πρώτων ιδεωδών κατά τρόπο ουσιαστικά μοναδικό.

**8.** Έστω $k$ ένα αλγεβρικά κλειστό σώμα και ανάγωγο $f \in k[x,y]$ της μορφής $f = ax + by + g$, όπου $g \in (x,y)^2$. Έστω $C_f$ η αντίστοιχη καμπύλη. Θέτουμε $R = k[C_f]$ και $P = (x,y)/(f)$ που είναι ένα πρώτο ιδεώδες του $R$. Αποδείξετε ότι η τοπικοποίηση $R_P$ είναι δακτύλιος διακριτής εκτίμησης $\Leftrightarrow a,b \neq 0 \Leftrightarrow$ το σημείο $(0,0)$ δεν είναι ιδιάζον.

# Βιβλιογραφία

Στις σημειώσεις αυτές χρησιμοποιήθηκαν τα παρακάτω βιβλία. Για παραπέρα μελέτης της Μεταθετικής Άλγεβρας, συνιστούμε τα [1], [2] και [3].


1. M.F. Atiyah and I.G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass, 1969.
2. D. Eisenbud, Commutative Algebra with a view toward Algebraic Geometry, Springer-Verlag, 1995.
3. H. Matsumura, Commutative Ring Theory, Cambridge 1986.
4. K. Ireland and M. Rosen, A. Classical Introduction to Modern Number Theory, Springer-Verlag, 1990.
5. M. Reid, Undergraduate Algebraic Geometry, Cambridge, 1988.
6. M. Raid, Undergraduate Commutative Algebra, Cambridge, 1995.
7. R.Y. Sharp, Steps in Commutative Algebra, Cambridge, 1990.
8. I. Shafarevich, Basic Algebraic Geometry vol I, Springer-Verlag, 1988.
9. I.N. Stewart and D.O. Tall, Algebraic Number Theory, Chapman and Hall, 1987.